平成２２年度医療情報化促進事業
（医療認証基盤整備事業）

－どこでも MY 病院構想及びシームレスな地域連携医療の実現に向けた実証事業－

成果報告書

平成２４年２月

センチュリー情報サービス株式会社

はじめに

- 本事業の位置付け
  政府 IT 戦略に基づいて、「どこでも MY 病院構想」や「シームレスな地域連携医療」のような疾病や地域の実情に合わせたシステムの開発が行われている。これらのシステムは機微な医療情報を扱うため、高度なセキュリティ対策が求められている。しかし、セキュリティ対策は、高度なスキルや開発工数が必要になるため、システム開発の負担になっている。このため、これらのシステムを構築する上で共通的なセキュリティ対策として、攻撃の頻度が高く、最も対策の効果が高い「なりすまし」に対して、厚生労働省の推進する HPKI 認証技術を適用した共通モジュールを開発し、「医療認証基盤システム」と共に提供する。
  「医療認証基盤システム」によって、医療認証サービスを全国規模で提供することにより、地域を超えたシステム連携が容易にできるようになる。また、医師以外の歯科医師・看護師・薬剤師等の医療従事者の認証も展開できる医療分野に普遍的な認証方式が構築できる。

目　　次

1. 本事業の背景と目的 1
1.1. 本事業の背景 1
1.2. 本事業の目的 3
2. 本事業の内容 4
2.1. 本事業の実施すべき内容 4
2.2. 実施するサービス 5
2.3. 構築するシステム概要 6
2.4. 実施体制とスケジュール 7
2.4.1. 実施体制 7
2.4.2. 実施スケジュール 9
2.5. 個人情報保護 13
2.5.1. 個人情報保護の方針 13
2.5.2. 個人情報管理体制 14
2.5.3. 個人情報保護の対象情報 15
2.5.4. 具体的な施策 16
3. 本事業の成果 17
3.1. 本事業により実現した成果 17
3.1.1. 実証内容と成果 17
3.1.2. 実現した効果 52
3.1.3. 成果指標の達成状況 53
3.2. 本事業により開発したシステム 70
3.2.1. 開発したシステムの全体像について 70
3.2.2. アプリケーションシステムへの組込み方法 72
3.2.3. 利用者管理方法 74
3.2.4. サービス利用方法 75
3.2.5. 運用方法 77
3.2.6. データセンタの運用基準 78
4. まとめ 79

添　付　資　料

SAML 実装仕様書

第Ⅰ編　概要、用語及び参考文献（第 1.0 版）

第Ⅱ編　フレームワーク（第 1.0 版）

第Ⅲ編　機能仕様（第 1.0 版）

第Ⅳ編　実装規約（第 1.0 版）

第Ⅴ編　試験仕様（第 1.0 版）

第Ⅵ編　セキュリティとプライバシに関する考慮事項（第 1.0 版）

1. 本事業の背景と目的

1.1. 本事業の背景

2010 年 5 月 11 日に内閣官房 IT 戦略本部から発表された「新たな情報通信技術戦略」では、「全国どこでも過去の診療情報に基づいた医療を受けられるとともに、個人が健康管理に取り組める環境を実現するため、国民が自らの医療・健康情報を電子的に管理・活用するための全国レベルの情報提供サービスを創出する。このため、第一段階として、個人が自らに対する調剤情報等を電子的に管理する仕組みを実現する。また、匿名化されたレセプト情報等を一元的なデータベースとして集約し、広く医療の標準化・効率化及びサービスの向上に活用可能とする仕組みを構築する」とされている。この「新たな情報通信技術戦略」の工程表にある「どこでも MY 病院構想」や「シームレスな地域連携医療」の実現は、 医療機関の間で診療情報を共有することによって、医師の正確な情報に基づいた高い精度の診断や医療機関の専門性を活用したチーム医療など、診療や治療に係るさらなる質的な向上が期待できる。

経済産業省では、この施策を受けて、患者がいつでもどこでも高品質の医療や介護のサービスが受けられる基盤を構築することを狙いとして、平成 22 年度サービス産業活動環境整備調査事業（医療等情報化共通基盤構築調査事業）を立ち上げている。この事業において、経済産業省より委託を受けた株式会社管理工学研究所がこれまでの標準化やセキュリティに関する成果を整理し、「平成 22 年度サービス産業活動環境整備調査事業（医療等情報化共通基盤構築調査事業）報告書」（以下、医療情報化共通基盤調査事業報告書）に今後構築する基盤のあるべき姿及び設計指針としてまとめてある。

医療情報化は、本事業の「どこでも MY 病院構想」や「シームレスな地域連携医療」のような疾病や地域の実情に合わせたシステムの構築が重要である。一方で、クラッカーが複数の攻撃を組合せてシステムの脆弱性に付け込んでアカウント情報を搾取したり、システムを破壊するなど、より複雑で悪質なサイバー攻撃が多発している。このため、情報の機微性の高い医療情報を扱うシステムには、高度なセキュリティ対策が求められている。

サイバー攻撃の中で最も多いものがアカウント情報の搾取による「なりすまし」である。このような攻撃に最も有効な技術として、厚生労働省の推進する保健医療福祉分野公開鍵基盤（以降、HPKI）がある。HPKI は、公開鍵と秘密鍵の二つの鍵を用いて電子署名、認証、暗号化、改ざん検知などの機能が提供できる技術を保健医療福祉分野向けに医師、薬剤師、歯科医師などの資格情報を確認できるように拡張したものである。HPKI は、「医療情報化共通基盤調査事業報告書」において活用すべきと指摘されている。

HPKI のようなサイバー攻撃に対して共通的なセキュリティ対策となるものは、日本の国としてバラバラに対策を立てるのではなく、標準的な対応方法や共通モジュールの提供が有用である。このため、標準化の必要性、統一されたセキュリティのあり方については、過去の事業の検証も踏まえ、厚生労働省の「医療情報システムの安全管理に関するガイドライン」や HPKI の CP/CPS 等にまとめられている。

しかし、これらの指針の存在に関わらず、現場の解釈によって、標準形式やセキュリティ対策が統一されているとは言いがたい現状がある。このため、全国で統一的な解釈に基づいたセキュリティ対策ができる環境の構築が望まれている。特に、患者の個人情報を扱う中心的存在である医師のなりすましを防ぐ、医療認証サービスに関する要望が特に高くなっている。

1.2. 本事業の目的

本事業は、患者（国民）の医療・健康情報の安全な交換、流通に寄与する共通モジュールやシステムを提供することが目的である。「どこでもMY病院構想」や「シームレスな地域連携医療」は、国民の医療・健康情報を取り扱うが、個々のシステムは疾病や各地域に閉じたシステムになっている。このため、これらのシステムを全国規模で運用しようとする場合、全国規模で医師の認証ができる認証基盤が必要となる。

本事業は、「どこでもMY病院構想」及び「シームレスな地域連携医療」のセキュリティ基盤として、以下のような医療認証サービスを提供する。

- 全国規模の認証を提供することで、国民の利便性向上を実現する。
- 国民の情報にアクセスしてよい資格者の確実な認証を実現する。

本事業では、HPKIを利用して医療認証サービスを提供する医療認証基盤システムの認証・認可の仕組みを構築する。HPKIに規定された資格情報は、システムの利用者として、患者情報を最もよく扱う医師に関する資格情報を用いでHPKIカードを用いた認証基盤を開発する。これにより、実証事業全体における開発や構築負荷を低減することが期待できる。

また、将来的には本事業の範囲だけに留まらず、他の医療従事者の資格情報や医療以外の全ての関係者や施設等の認証基盤を提供することも想定して検討する。例えば、政府で検討されている社会保障・税の共通番号制度やIT戦略本部で検討がなされている国民ID等との関係や、チーム医療のような医療職種間や医療と介護等における関係などとの整理が必要と考える。本事業の成果については、厚生労働省や関連する学会、工業会等の団体との連携を検討することで、医療情報化に際し、広く利用されるものを目指す。

2. 本事業の内容

2.1. 本事業の実施すべき内容

HPKI は、保健医療福祉分野における認証基盤として厚生労働省が推進している。しかし、HPKI の必要性とは別に、一般的な電子証明書に hcRole という資格情報が追加されている。現状は、HPKI に係る認証機能をシステム毎に開発する必要がある。このため、資格情報に係るシステムの開発や基盤整備が普及の課題となっている。

本事業では、HPKI に対応した医療認証基盤システム及び SAML 連携モジュールを共通モジュールとして開発する。これにより、HPKI の共通認証基盤環境が整備でき、資格情報に係る HPKI 関連のシステムの開発や基盤整備が必要なくなり、「シームレスな地域連携医療」や「どこでも My 病院」などの医療情報システムの構築が簡便になる。また、アセスメントされた信頼できるセキュリティ対策が施された共通モジュールを組込むことにより、医療者の資格者認証がどの地域でも一定のセキュリティの上に提供することができるようになる。

2.2. 実施するサービス

日本医師会認証局が発行する認証用の証明書が格納された HPKI カードを用いて医師資格を確認する医療認証サービスを提供する。これにより、以下のようなことが可能になる。

- 医師は認証に用いた Security Assertion Markup Language (SAML)のアサーションを用いて、患者の既往歴や服薬情報の検索、過去の診療履歴の確認など、様々な医師向けのサービスを利用することができる。SAML は、シングルサインオンやサインドチケットなど、認証に関わる様々な用途に使えるアサーションの記述方法や伝送方法を規定するプロトコルである。
- アプリケーション側では、個別に医師資格確認のための認証サービスシステムを構築する必要がなくなる。

将来を鑑み、本事業の医療認証基盤システムと、既存の認証システムとの連携や統合を考慮する。このため、システム間の相互運用性を担保するため、「SAML 実装仕様書」としてシステム間のプロトコル仕様を厳密に定義したドキュメントを作成する。また、認証サービスシステムの普及・拡大を狙いとして、本事業で開発した共通モジュール、SAML 連携モジュールをシステムに組込むための取扱説明書を提供する。

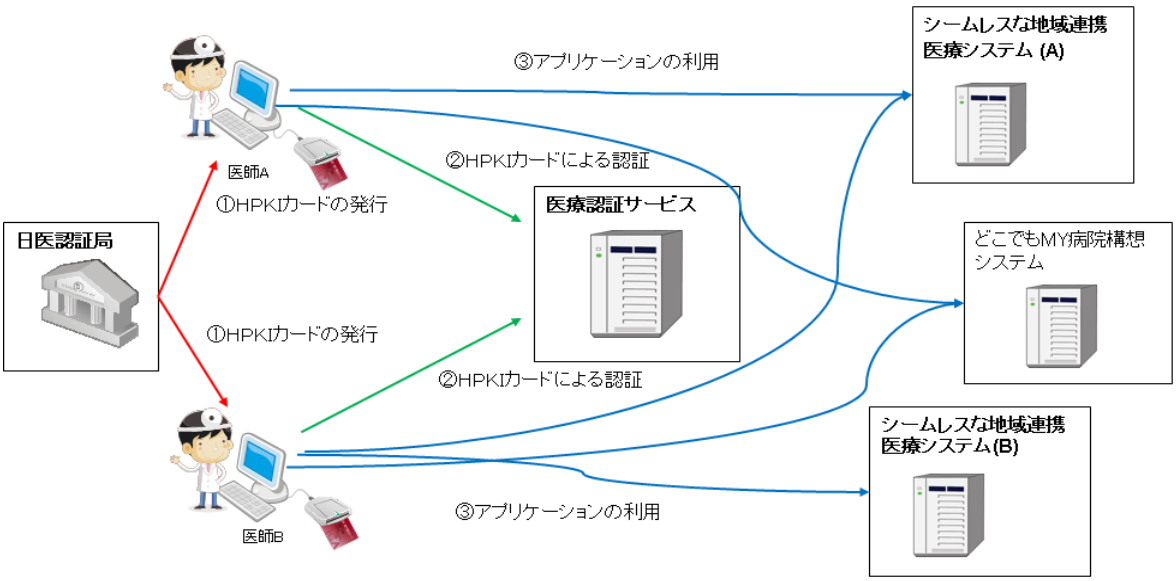


図 2.2-1 サービスの概要

2.3. 構築するシステム概要

どこでも MY 病院構想やシームレスな地域連携医療システムの中で、医師の資格を確認する認証部分を共通化する。

本提案範囲では、まず医師の認証を対象として事業を行う。事業終了後に患者やその他の医療関係者に対する認証部分と連携可能なシステムへの展開を考慮する。

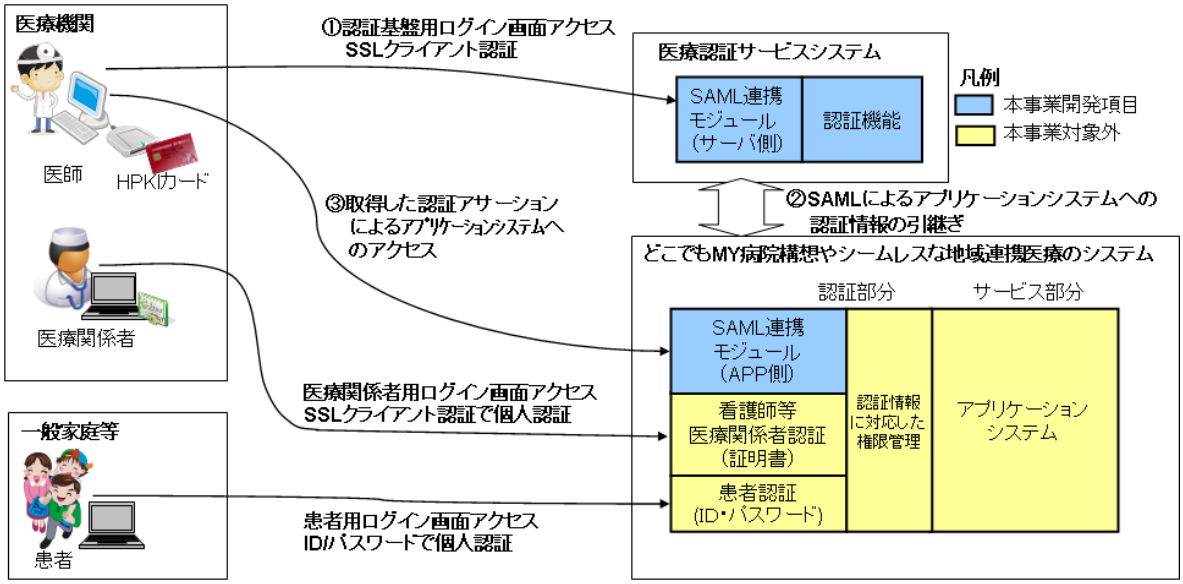


図 2.3-1 システム概要

2.4. 実施体制とスケジュール

2.4.1. 実施体制

コンソーシアムの体制図を図 2.4.1-1 に示す。

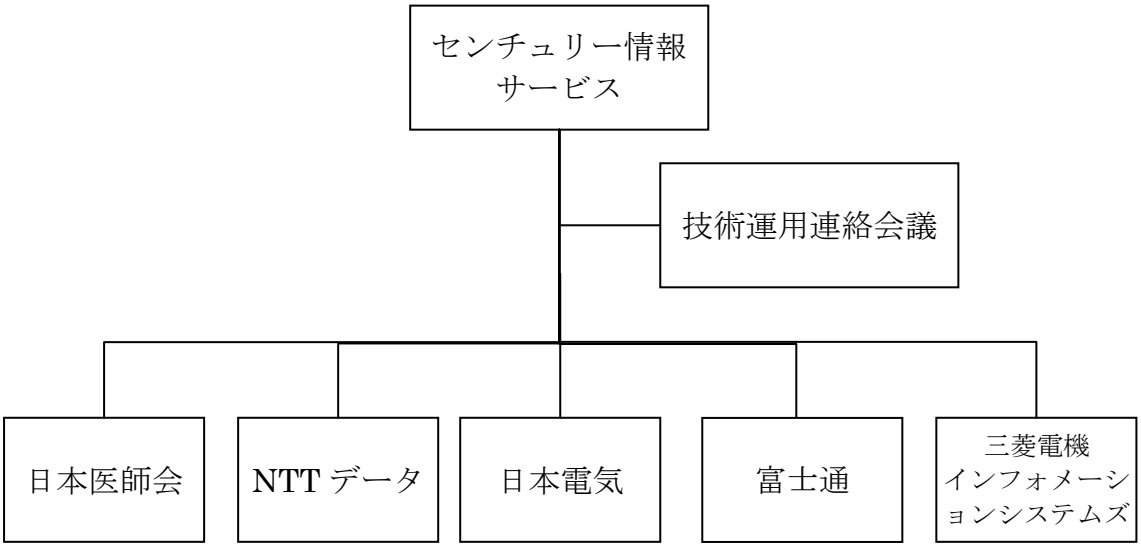


図 2.4.1-1　コンソーシアムの体制図

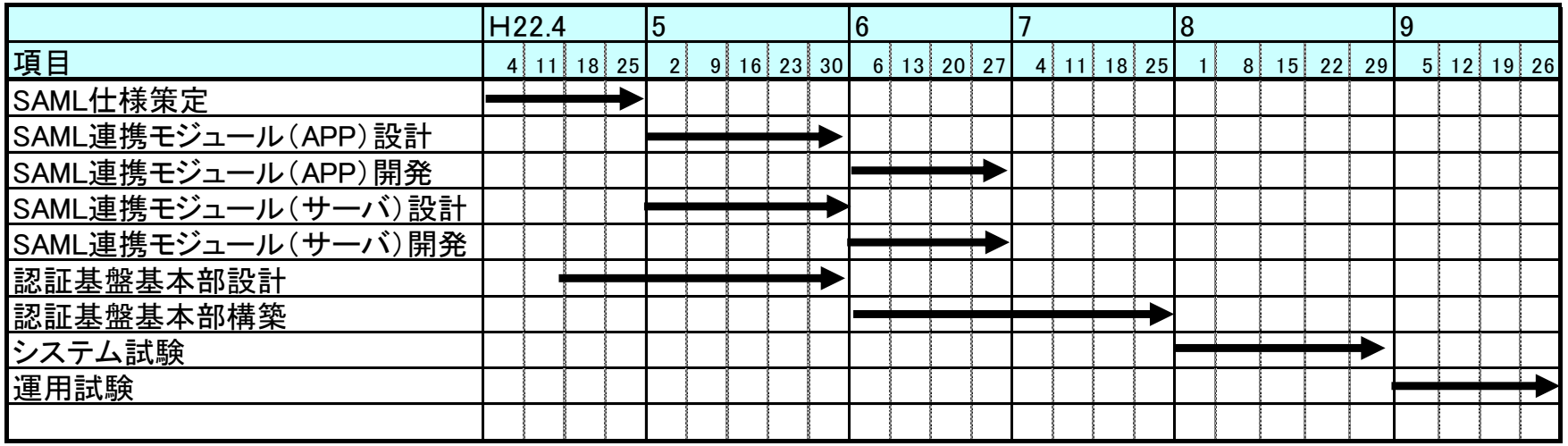
コンソーシアムに参画するメンバの役割を表 2.4.1-1 に示す。

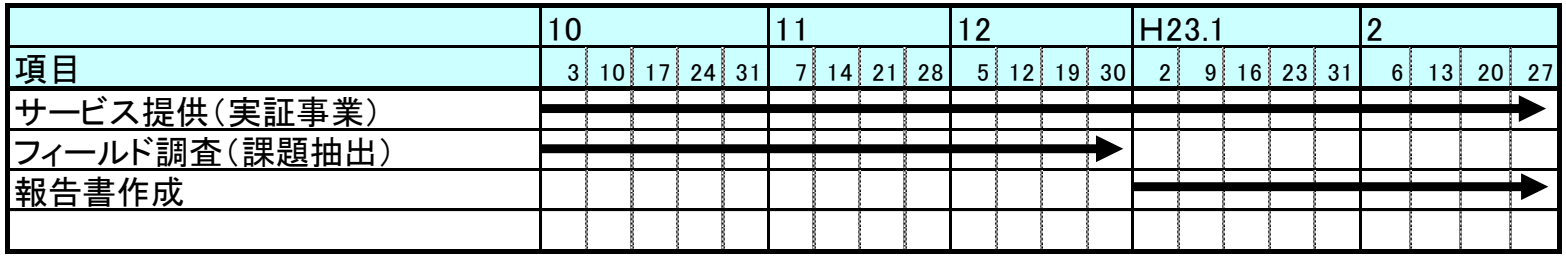
表 2.4.1-1　コンソーシアム参加メンバの役割

組織名	役割
センチュリー情報サービス	コンソーシアムの全体取りまとめ 技術運用連絡会議の運営
日本医師会	日医認証局の運用及び HPKI カードの発行 医療認証基盤システムの運用
日本電気	SAML 認証連携モジュール（APP 側）の設計および開発
三菱電機インフォメーションシステムズ	SAML 認証連携モジュール（APP 側、サーバ側）の設計および開発 医療認証基盤システムの構築
NTT データ	SAML 認証連携モジュール（APP 側、サーバ側）の設計支援
富士通	

2.4.2. 実施スケジュール

本事業の実施スケジュールは以下のとおりである。





本事業では、実施スケジュールを遵守して設計を円滑に進めるため、以下のような会議を作って事業を推進した。

（1） 技術検討 WG

技術検討 WG は、以下の内容についてコンソーシアムのメンバで技術的な検討及び取りまとめを行った。

- SAML 実装仕様書の設計とドキュメント化
- SAML 試験仕様の設計と相互運用試験
- SAML 連携モジュールの取扱説明書の作成
- 具体的な実証及び評価の取りまとめ

技術検討 WG の実施日程は以下の通りである。

開催	日程	時間
第 1 回	2011/4/15 （金）	13:30-15:30
第 2 回	2011/4/25 （月）	15:00-17:30
第 3 回	2011/5/6 （金）	9:30-11:30
第 4 回	2011/5/12 （木）	15:00-18:00
第 5 回	2011/5/13 （金）	15:00-17:00
第 6 回	2011/6/6 （月）	13:00-16:00
第 7 回	2011/6/15 （水）	10:00-12:00
第 8 回	2011/6/22 （水）	13:00-15:30
第 9 回	2011/7/6 （水）	15:00-17:00
第 10 回	2011/7/20 （水）	15:00-17:00
第 11 回	2011/7/27 （水）	15:00-17:30
第 12 回	2011/8/10 （水）	10:00-12:30
第 13 回	2011/8/31 （水）	14:00-17:30
第 14 回	2011/9/26 （月）	15:00-19:30
第 15 回	2011/10/12 （水）	15:00-17:00
第 16 回	2011/10/19 （水）	15:00-18:00
第 17 回	2011/11/9 （水）	15:00-17:30
第 18 回	2011/11/16 （水）	15:00-17:00
第 19 回	2011/12/7 （水）	15:00-17:00
第 20 回	2011/12/21 （水）	15:00-17:30
第 21 回	2012/1/18 （水）	15:00-16:30
第 22 回	2012/1/30 （月）	16:00-17:00

（２） 医療認証基盤技術運用連絡会議

技術検討 WG は、以下の内容について、医療分野や認証に関する専門家をメンバにして技術的な検討及び取りまとめを行った。

- SAML 実装仕様書のセキュリティアセスメント
- SAML 実装仕様書の継承性の検証
- SAML 実装仕様書の有用性
- 本事業の目標管理に関するアセスメント

技術検討 WG の実施日程は以下の通りである。

開催	日程	時間
第 1 回	2011/9/2 （金）	14:00-16:00
第 1 回技術 WG	2011/9/29 （木）	14:00-16:30
第 2 回技術 WG	2011/10/31 （月）	14:00-16:00
第 2 回	2011/12/5 （月）	14:00-15:00
第 3 回技術 WG	2012/1/10 （火）	14:00-15:00
第 3 回	2012/1/30 （月）	14:00-15:30

（３） 普及拡大のための説明会

普及拡大のための説明会の実施日程は以下の通りである。

開催	日程	時間
SAML 勉強会	2011/7/22 （金）	15:00-17:00
SAML 連携モジュール説明会	2011/12/19 （月）	17:00-18:00

（４）本事業に進捗管理及び技術情報を共有する場

本事業に進捗管理及び技術情報を共有する場として開催された下記の会議に参加した。

- 推進委員会
- システム WG
- 報告会

① 推進委員会

開催	日程	時間
第 1 回	2011/4/20 （水）	15:00-17:00
第 2 回	2011/9/20 （火）	14:00-18:30
第 3 回	2011/12/22 （木）	16:00-18:00

② システムWG

開催	日程	時間
第 1 回	2011/4/20 （水）	17:30-19:30
第 2 回	2011/5/6 （金）	13:00-16:00
第 3 回	2011/6/1 （水）	14:00-17:00
第 4 回	2011/6/8 （水）	14:00-17:00
第 5 回	2011/7/4 （月）	14:00-17:00
第 6 回	2011/7/22 （金）	10:00-13:00
第 7 回	2011/8/3 （水）	14:00-17:00
第 8 回	2011/8/18 （木）	13:00-16:00
第 9 回	2011/9/8 （木）	14:00-17:00
第 10 回	2011/11/15 （火）	10:00-13:00
第 11 回	2011/12/19 （水）	14:30-17:00
第 12 回	2012/1/25 （水）	10:00-13:00

③ 報告会

開催	日程	時間
中間報告会	2011/10/26 （水）	13:00-17:00
最終報告会	2012/2/14 （火）	13:00-17:30

2.5. 個人情報保護

2.5.1. 個人情報保護の方針

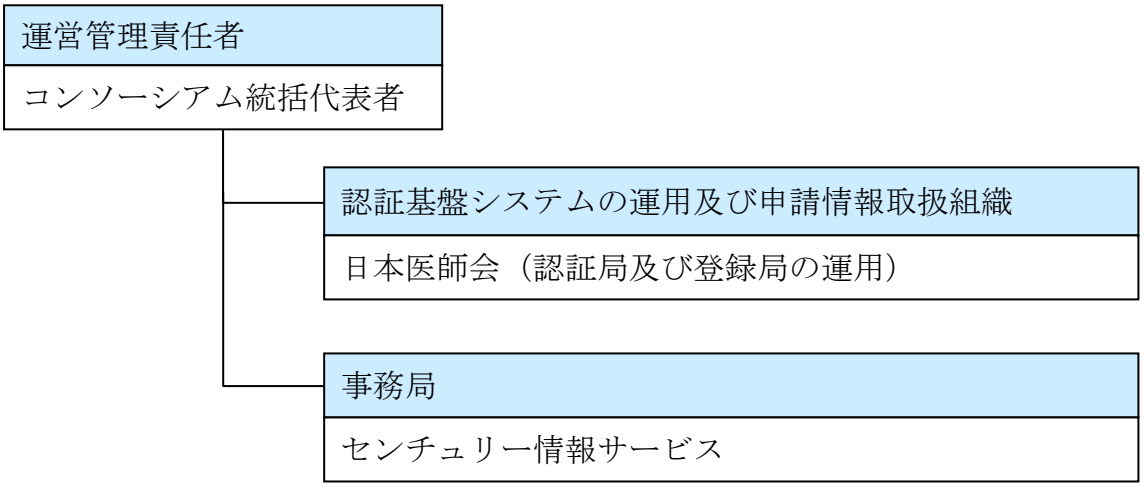
本事業における個人情報保護に関する方針を以下に示す。

- 本事業で利用者から提供された個人情報は、本事業の用に供する以外は使用しない。
- 利用者から提供された個人情報を本事業に利用するために、利用者から予め同意を得るものとする。(包括同意を含む)。また、本事業の利用用途以外で利用する場合も、利用者本人に対して予め本人の同意を得るものとする。
- なお、本事業における医療認証基盤システムを利用するためには、日医認証局の HPKI カードを持っていることを前提としていることから、実証期間中に関しては、日医認証局の申込時点で利用者同意を得る方策も検討する。
- 利用者から提供された個人情報は、法の要請による開示を除き、本コンソーシアム以外の第 3 者に提供しない。
- ただし、利用者本人から個人情報開示申請がある場合は利用者本人にのみ開示する。
- 個人情報の取り扱いを外部に委託する場合は、本実証事業体の個人情報保護の基準に従った十分な保護措置が行われること（プライバシマーク、情報セキュリティマネジメントシステム等）を確認のうえ選定する。

2.5.2. 個人情報管理体制

本事業における個人情報保護に関しては以下のような体制で管理する。

- 各実施部門は情報セキュリティに関する事象を発見又は発生した場合には、運営管理責任者へ速やかに報告する。
- 報告を受けた運営管理責任者は速やかに処理するとともに、処置の記録を作成する。
- 事務局は情報セキュリティに関する事象が発生した際に、処置が円滑に実施されるように支援する。



2.5.3. 個人情報保護の対象情報

本事業において、個人情報保護の対象と考えられる情報は、医療認証基盤システムの利用申込に必要な以下の情報である。

- 利用者氏名
- 医籍登録番号

2.5.4. 具体的な施策

- 本事業に参加する団体の個人情報保護方針等を踏まえ、利用目的等が明示されたコンソーシアムにおける個人情報保護方針を策定する。
- サービス提供時には事前に利用者に個人情報保護方針を配布するなど対策を行う。
- サービス設計に際して、不必要な個人情報を取得しないことに留意し、情報漏えい等のリスク対策を講じる。
- 個人情報については、許可された者以外がアクセスできないような措置等を講じ、個人情報への不正アクセス又は漏洩が発生しないよう適切に管理する。
- 個人情報の取扱いについては、運営要員を対象とし、各運営要員の役割に応じた教育・訓練計画を策定し教育及び訓練を行う。
- 個人情報漏洩や苦情及び相談への対応、並びに開示等の求めに対しては、窓口を明示して速やかに対応する。

3. 本事業の成果

3.1. 本事業により実現した成果

3.1.1. 実証内容と成果

（1）実証内容

全国規模で資格者を確実に認証するため、認証機能を一元化するため、下記のようなことを実証的に検証した。

(a) 相互運用性の実証

① 本コンソーシアムの参画ベンダ 4 社が協同で、相互運用性が確保できるレベルの「SAML 実装仕様書」を規定した。

② 2 社において、「SAML 実装仕様書」に基づいて実装し、相互運用試験を行って、相互運用性が確保できることを確認し、「SAML 実装仕様書」によって相互運用性が確保できることを実証した。

(b) SAML 連携モジュールの実用性・安全性の実証

① 下記 3 事業において実装していただき、機能及び性能が十分であることを実証した。

- のとの私の MY 病院事業
- 小児疾患連携医療事業
- 周産期小児健康情報 NW 事業

② 「技術運用連絡会議」において、セキュリティアセスメント等の技術的な評価を行い、SAML 連携モジュールの安全性について検証した。

(c) 連携モジュールの普及に向けた実証

① 各サイトや今後の利用拡大に必要となる、システムを導入するための「取扱説明書」他の導入に関わる資料を作成し、各サイト向けに情報を提供した。本導入に関わる資料は、接続試験及び本運用時の接続設定に係る情報が記載されており、DOS 攻撃等のネットワークの脅威を避けるために非公開とする。

② 「導入に関わる資料」に基づいて上記 3 事業で実装し、3 地域における実証において技術的、運用的な問題が起きないことを実証した。

（２） 実証の具体的な成果

(a) 開発物の標準化

① HTTP over SSL/TLS 環境において通信異常が発生した場合のシステムの対象方法を明確にするため、「SAML 実装仕様書　第Ⅲ編　機能仕様」に実装に当たって検討したプロトコル要素の仕様、通信状態遷移図、正常・異常に関わる通信シーケンスを機能仕様として記載している。

② 仕様に関する曖昧さを排除するため、「SAML 実装仕様書　第Ⅳ編　実装規約」において、実装した SAML のパラメータに関するサンプルを仕様に例示してある。

③ 医療認証基盤システムと接続する際の単体試験、及び共通モジュール相当の機能を独自に開発する場合の結合試験仕様として使用できるように、「SAML 実装仕様書　第Ⅴ編　試験仕様」において、共通モジュールの試験仕様に関わる情報を仕様に例示してある。

④ 「SAML 実装仕様書　第Ⅲ編　機能仕様」において、汎用的な仕様の HTTP、SOAP、SSL/TLS を SAML の実装に必要な項目に絞って用法を詳細に記載している。

⑤ 「SAML 実装仕様書　第Ⅲ編　機能仕様」において、オープンソースのソフトウェアを利用して開発できるように、通信における入出力インタフェースを定義している。

⑥ 「SAML 実装仕様書　第Ⅴ編　試験仕様」において、医療認証基盤システムにおける相互運用性の確保を確認するために最低限必要な試験方法について記載している。

(b) 開発物の継承性

① 経済産業省「平成 22 年度医療情報化促進事業」の参画メンバに対して、本実装仕様書についての説明会を開催している（１回目：2011/7/22　、２回目：2011/12/19）。

② 「医療認証基盤技術運用会議」を開催して、医療・認証分野に関係する団体・有識者に参集いただき、セキュリティアセスメントや内容に関するコメント等の意見集約を実施している。

③ 標準化団体に対して、今後実装に関わる提案ができるように、SSL/TLS のクライアント認証を使用した具体的な実装事例として、プロトコル要素、通信状態遷移図、通信シーケンス等の機能仕様を明確化している。

④ 中央省庁の間で開発した技術内容を共有できるように、本実証事業に関するドキュメントを WEB 等用いて公開する予定である。
⑤ システム開発や構築が容易になるように、「SAML 連携モジュール(APP)利用の手引き」において、サンプルソース等を掲載して、組込み方法が具体的に分かるように解説している。
⑥ 導入に関わる資料として、提供する共通モジュール毎に、「SAML 連携モジュール(APP)利用の手引き」(日本電気)、「SAML 連携モジュール(APP) 導入ガイド」(三菱電機インフォメーションシステムズ)を用意して、導入に関わる申請作業や技術的な対処手順を解説している。また、これらに関する説明会を開催している。

(c) 開発物の性能・安全性
① SAML の実装設計に当たって、「SAML セキュリティとプライバシについての考慮事項」を和訳して「第VI編　セキュリティとプライバシに関する考慮事項」として SAML に関して考察されたセキュリティの考慮事項を明確にしている。
② 「第VI編　セキュリティとプライバシに関する考慮事項」に基づいてセキュリティ上の脅威と SAML における対処案を参考に表 3.1.1-1 に示すような評価シートを作成し、SAML の実装状況を評価している。
③ 「医療情報システムの安全管理に関するガイドライン」で参照されている HEASNET の「『医療情報システムの安全管理に関するガイドライン』の実装事例に関する報告書」で提唱され、レセプトオンラインに用いられているオンデマンド VPN の適合性評価に使用されている「HEASNET のチェックシート」を用いて IDP のシステム環境のセキュリティについて評価している。
④ 「SAML 連携モジュール(APP)利用の手引き」(日本電気)にあるログの実例の時間から性能は下記のようになっている。
(i) レスポンスタイム＝0.058 秒
※ SAMLArt の受信から ArtifactResponse の受信・解析まで
(ii)ターンアラウンドタイム＝0.071 秒
※ リソース要求（カードアクセス・PIN 入力を除く）から ArtifactResponse の受信・解析まで

(d) 開発物の経済性
① SAML 仕様の理解や機能設計・詳細設計の参考事例として、「SAML

実装仕様書　第Ⅳ編　実装規約」に SAML パラメータのサンプルデータを載せて解説している。

② 詳細設計や試験仕様の設計の機能項目などの抽出の参考事例として、「SAML 実装仕様書　第Ⅴ編　試験仕様」に開発した共通モジュールの結合試験仕様をサンプルとして載せて解説している。

③ 地域毎に異なるシステム要件を考慮して、API 型（日本電気）と AP 型（三菱電機インフォメーションシステムズ）の 2 種類の共通モジュールを開発して、システムの要件に合せて選択的に導入できるようにしている。

④ 日本医師会に置かれた認証局から発行された公開鍵証明書を用いて医師の本人性や資格が確認できる。これによって、地域内だけでなく、システムに登録されていない地域外の医師の本人確認及び資格確認ができるようにしている。

(e)　開発物のセキュリティアセスメント

SAML 実装仕様書で規定した実装方法について、実装の範囲や技術的な内容、及びこれらのセキュリティ的な対策について整理する。ネットワークの脅威と SAML で検討された対策に対する対応について表 3.1.1-1 に示す。SAML の下位レイヤである SSL/TLS の脆弱性とその対策について表 3.1.1-2 に示す。

表 3.1.1-1 ネットワークの脅威と SAML で検討された対策に対する対応

脅　威	内　容	対　策	対応状況
6.1.1 盗聴	伝送路の機密性に関する要件が存在しない場合、盗聴の当事者は要求とこれに対応する応答の S 両方の OAP メッセージを取得することが可能である。この盗聴は、1 つ以上のアサーションを含む要求と応答の内容の両方が明らかにされる。 要求内容の漏えいは、誰からどのようなアサーションが要求されているか明らかになるため、要求側のセキュリティを脆弱なものにする。例えば、サイト X がサイト Y に対して頻繁に所定の確認方法を含む認証アサーションを要求していると判断できる場合、盗聴者はサイト X のネゴシエーション情報を使用できる可能性がある。 同様に、一連の認可クエリに対する盗聴によって、指定された認可オーソリティの管理下にあるリソースのマップが作成できる。 さらに、要求自体の漏えいがプライバシの侵害を発生させる場合がある。例えば、クエリとその応答に関する盗聴は、特定の利用者が医療情報サイト、政治的なサイトなどの漏らすべきでない情報がある照会サイト上でアクティブであることを	このようなリスクが懸念される場合、盗聴攻撃に対して、伝送中のメッセージに機密性を提供するいくつかの方策が提供されている。 SOAP メッセージの場合、この機密性は、SOAP レベルまたは SOAP の伝送（またはそれより下の)レベルのいずれかで対処することができる。SOAP レベルで伝送中の機密性を保つとは、そのような SOAP メッセージを構築することを意味する。SOAP の伝送に関係なく、目的の当事者以外の誰もメッセージにアクセスできないにすることである。 この問題に対する一般的な解決策は、ほとんど XML 暗号化である。この仕様は、SOAP メッセージ自体の暗号化を許している。これにより、暗号化の鍵が危殆化されている限り、SOAP メッセージの盗聴の危険性を排除している。他方、利用者は伝送中の機密性の提供を SOAP の伝送層、または下位層に依存することができる。 機密性を提供する方法は、SOAP の伝送方法の選択に依存する。 HTTP を TLS/SSL で使用するのも一つの方法であ	○ （HTTPS+SOAP 通信）

脅　威	内　容	対　策	対応状況
	公開することがある。また、応答で伝送されるアサーションの内容は、機密性を守るべき情報である。これは、属性アサーションを含む応答にとって特に留意すべき事項である。これらの属性が(信用格付け、医療の属性など)交渉の当事者でないエンティティに公開されるべきでない情報の場合、盗聴のリスクは高くなる。	る。他の伝送方法では、伝送中の機密性を保証する他の技術が必要とされる。例えば、SMTP では S/MIME を使用する。SOAP の下位層で伝送中の機密性を提供する場合がある。例えば、要求・応答の会話が IPsec トンネルで行われる場合、伝送中の適切な機密性は、トンネル自体によって提供される。	
6.1.2 リプレイ	SOAP バインディングのレベルでのリプレイ攻撃のための小さな脆弱性が存在する。リプレイ攻撃は、様々なプロファイルで問題になる。SOAP バインディングレベルでのリプレイ攻撃に関する主な懸念事項は、DOS 攻撃の方法としてリプレイ攻撃の使用に関する可能性である。	リプレイ攻撃を防ぐ最善の方法は、一般的に、最初の場所でメッセージのキャプチャを防ぐことである。伝送の機密性で提供するために使用されるトランスポートレベルのスキームの一部は、この目標を達成する。例えば、SAML 要求・応答の会話が HTTP/TLS と組み合わせた SOAP で行われている場合、第三者によるメッセージ挿入を防止することができる。	○ (HTTPS＋SOAP 通信)
6.1.3 メッセージの挿入	作成された要求または応答が、メッセージストリームに挿入される。認可決定クエリに対する偽の「承認」の応答のような偽の応答または属性クエリに対する応答の偽の属性情報の返却は、受信者に不適切なアクションを起こさせる可能性がある。	要求を挿入する機能は、SOAP バインディングレベルではではない。偽の応答を挿入するは、DOS 攻撃に用いることができる。例えば、応答のために SOAP エラーを返す。しかし、この攻撃はすぐに明らかになる。作成された応答を返却するより微妙な攻撃は、各 SOAP 応答はエラーの場合を除いて SAML プロトコル応答	○ (InResponseTo 使用)

脅　威	内　容	対　策	対応状況
		が一つでなければならないという SOAP バインディングの定義に基づいた、適切な SAML プロトコルに仕組まれる。SAML プロトコルは、2 つの機構でこの問題に対処する。必須属性の InResponseTo を用いた要求と応答の対応付けは、応答を生成するために要求を傍受しなければならないので攻撃を難しくする。発信者認証は、署名された SAML 応答または SSL / TLS のようなセキュアなトランスポート接続によって行われる。	
6.1.4 メッセージの削除	メッセージ削除攻撃は、レスポンダに到達する要求を妨げる、または要求者に到達する応答を妨げる。	SOAP バインディングは、このいずれの場合にも対処していない。要求と応答メッセージの対応付けは、一般的に、このような攻撃を阻止することができる。例えば、StatusResponseType の InResponseTo 属性の使用である。	○ (InResponseTo 使用)
6.1.5 メッセージの変更	メッセージの変更は、SOAP バインディングの両方向へのである。 要求の内容を置き換えた要求の変更は、著しく異なる結果が返される可能性がある。この結果は、巧妙な攻撃者によってアサーションに基づいて動作するシステムを侵害するために適宜使用することができる。例えば、<Attribute>要素に要求	これらの潜在的なに対処するため、伝送中のメッセージ完全性を保証するシステムを使用する必要がある。SAML プロトコルと SOAP バインディングは、伝送中のメッセージ完全性を保証するシステムの導入を要求も禁止もしない。しかし、この大きなに起因して、このようなシステムを使用することを強く勧める。	△ SSL で伝送中のデータのみ暗号化して完全性を保つ

脅　威	内　容	対　策	対応状況
	された属性のリストの変更は、レスポンダによって要求の折衝や拒絶につながる結果を生むことができる。 要求の見かけの発行者を置換する要求の変更は、サービスの拒否や応答の不正確なルーティングにつながる可能性がある。この置換は、SAML の下位レベルで発生するものであり、スコープ外になっている。 アサーションの内容を置換する応答の変更は、折衝のあらゆる場面で発生する可能性がある。認証または認可決定の内容を置換する簡単な例は、非常に深刻なセキュリティ侵害につながる可能性がある。	SOAP バインディングのレベルでは、システムで要求と応答に XML 署名のように電子的に署名することによって行うことができる。SAML の仕様で、このような署名を認めている。詳細については、「SAML アサーション及びプロトコル仕様書」を参照してください。 受信者は、(第 4.4 節に示す賢明な鍵管理インフラストラクチャで)メッセージが電子的に署名されている場合、使用した鍵が侵害されていない限り、メッセージが伝送中に改ざんされていないことが保証される。 伝送中のメッセージの完全性は、SOAP のトランスポートの使用によって低レベルの目標を達成することができる。SOAP トランスポートは、完全性を保証するプロパティを提供するか、そのようなプロパティを提供するプロトコルに基づいている。SOAP over HTTP over TLS/SSL は、そのような保証を提供するトランスポートである。 暗号化だけでは、これに対する保護にならない。傍受したメッセージを変更できなくても、メッセージを別の新しいものと置換えることができる。	

脅　威	内　容	対　策	対応状況
6.1.6 中間者	SOAP バインディングは、中間者攻撃を受けやすい。あるエンティティが(盗聴やメッセージ変更の両方のセクションで説明したすべての危険を持つ)中間者として動作することを防ぐため、何らかの二者間の認証が要求される。	双方向の認証システムは、当事者相方に彼らの通信が実際に相手から来た通信であることを判断できるようにする。 この目標は、SOAP バインディングレベルでは、(上記 6.1.5 項で説明したすべての警告を含めて)要求と応答の両方にデジタル署名することによって達成できる。この方法は、真ん中にあって両方向に転送するために盗聴者を防ぐことはできない。しかし、検出されることなく任意の方法で通信内容を変えることは防止できる。 この作成者の認証は、SOAP の多くの AP がセッションを使用しないので、(送信者の認証とは対照的に)「盗聴者」としての「中間者」の弱点を防ぐために、送信者と作成者が同じであることを確認するためのトランスポート層からの情報を組合せることが必要になる。 別の実装は、下位層が提供する、または実装されている双方向の認証を提供する SOAP トランスポートに依存している。この例としては、サーバ側とクライアント側両方の証明書が必要な TLS/ SSL 上の HTTP を介した SOAP がある。 また、アサーションの有効期間は、中間	△ SSL サーバ認証のみ実施。SP 側は FW の IP アドレス認証を実施。

脅　威	内　容	対　策	対応状況
		者攻撃からのリスクの度合いの調整機能を提供する。アサーションの有効なウィンドウが短い程、傍受された場合の傷をより小さくできる。	
6.2.1 DOS	ターゲットの IDP または SP に悪意のあるリダイレクトを送信する。いかがわしいエンティティは、利用者エージェントにリダイレクト発行できる。これにより、利用者エージェントは、シングルサインオンを妨害するリソースにアクセスする。例えば、攻撃者は、利用者をすべての既存の認証セッションからログアウトさせるために、SP のログアウトリソースを利用者エージェントにリダイレクトすることができる。	副作用を起こすリソースへのアクセスは、現在の認証セッションに対応付けされた一時的な修飾子で指定することができる。また、確認ダイアログは、同じような意味を持つ一時的な修飾子を介して口を挟むことができる。	－
6.3.1 盗難アサーション	盗聴者が実際の利用者の SAML 応答とその中のアサーションをコピーできる場合、盗聴者は適切な POST のボディを構築し、送信先サイトで利用者を詐称できる。	機密性は、サイトと利用者ブラウザ間で応答がやり取りされるたびに適用しなければならない。これは、アサーションを取得する盗聴者に対する実際の利用者の SAML 応答を保護する。盗聴者に対する機密性を確保するため、破られた場合に備えて以下のような対応が必要である。 ・IDP と SP のサイトは、両方のサイトのクロックの設定が最大でも数分であることを確認するための合理的な努力をする必要がある。時刻同期のサービスの	△ アサーションの有効期間(１分)チェックあり、時刻同期なし

脅　威	内　容	対　策	対応状況
		多くは、インターネット上、または特定のソースのいずれかで利用できる。 ・非 SSO SAML プロファイルが POST バインディングを使用するとき、受信側がタイムリーに利用者の確認を行うことができることを保証しなければならない。この目的のために、利用者の SAML の認証アサーションは、POST されたフォームの応答に含まれなければならない。 ・SSO アサーションの NotBefore と NotOnOrAfter 属性の値は、IDP から SP のサイト間でアサーションが正常に交換できる最短の有効期間にすべきである。これは、数分というオーダが典型的である。これは、盗まれたアサーションが、わずかな時間の間しか正常に使用できないことを保証する。 ・SP サイトは、IDP サイトから取得したすべてのアサーションの有効期間をチェックし、期限切れのアサーションを拒絶しなければならない。SP サイトは、アサーションの IssueInstant または AuthnInstant 属性の値がアサーションを SP サイトで受信してから数分以内となるような SSO アサーションに対す	

脅　威	内　容	対　策	対応状況
		る有効性の厳格なテストを実装することを選ぶことができる。 ・SP サイトは、受信した認証ステートメントが利用者の IP アドレスを持った<samlSubjectLocality>の要素を含む場合、認証ステートメントに含まれている IP アドレスとブラウザの IP アドレスをチェックすることができる。	
6.3.2 中間者攻撃	SP サイトは、HTML フォームによって利用者からのベアラの SAML アサーションを取得する。このため、悪意のあるサイトがいくつかの新しい SP サイトで利用者を偽装することができる。新しい SP サイトは、悪意のあるサイトがアサーションの対象になると考えた方がよい。	SP サイトは、SAML 応答の受信者の属性が https//<アサーションの使用者のホスト名とパス>と一致していることをチェックしなければならない。応答がデジタル署名されている場合、悪意のあるサイト受信者の値を変更することはできない。	－ Artifact による SP サイトへの直接アクセスであることと、SP での中継は今回対象外となっている。
6.3.3 偽造アサーション	悪意のある、利用者またはブラウザの利用者は、SAML アサーションを偽造または変更することができる。	ブラウザ/POST プロファイルは、署名付き SAML アサーションを運ぶ SAML 応答が必要である。これにより、メッセージの完全性と認証の両方を提供する。SP サイトは、署名検証及び発行者の認証を行わなければならない。	－ Atrifact プロファイルのみ実装
6.3.4 ブラウザ状態の漏えい	ブラウザ/POST プロファイルは、Web ブラウザから SP サイトへのアサーションのアップロードを含んでいる。この情報は、Web ブラウザの状態の一部として利用可能であり、通常は利用者のシステム	このプロファイルを用いて通信されるアサーションは、常に寿命を短くして SAML アサーションの<Conditions>要素として<OneTimeUse>持たせるべきである。SP サイトには、アサーションが再	○ (アサーションの有効期間＝1 分)

脅　威	内　容	対　策	対応状況
	のストレージに完全に保護されていない方法で継続的に格納されている。ここでの脅威は、アサーションが後で「再利用」される可能性である。	使用されないようにすることが期待されている。	
6.3.5 リプレイ攻撃	リプレイ攻撃は、保護されたリソースに不正にアクセスするため、フォームの再送信を繰り返す。	プロファイルは、リプレイ攻撃の成功を防止する、転送されたアサーションの SP サイトでの 1 回使用の原則を義務付けている。	－
6.3.6 状態情報の変更または漏えい	一部のメッセージが改ざんまたは生成されたリレー状態を<RelayState>要素で伝送する。<RelayState>要素は、作成者による完全性の保護が推奨、機密性の保護がオプションになっている。攻撃者は、これらの条件が満たされていない場合、望ましくない行動を引き起こす可能性がある。さらに、正当なシステムエンティティは、この要素の値が機密保護されていないことによって、IDP または受動的な攻撃者に誤って情報を公開する可能性がある。	機密性と完全性が保護する中継状態データは推奨に従って設定する。この要素の値は、同じシステムエンティティによって生成・使用されるため、対称暗号化の基底が利用することを注記しておく。	○ (RelayState 使用)
6.4.1 盗難アーティファクト	盗聴者は、実際の利用者の SAML アーティファクトをコピーできる場合、実際の利用者の SAML アーティファクトで URL を作成し、送信先サイトで利用者を偽装することができる。	機密性は、サイトと利用者ブラウザ間でアーティファクトがやり取りされる都度、提供しなければならない。これは、盗聴者が実際の利用者の SAML アーティファクトへのアクセスを取得することに対する保護を提供する。	△ アサーションの有効期間(１分)チェックあり、時刻同期なし

脅　威	内　容	対　策	対応状況
		盗聴者が機密性を保護するために用いる対策を破った場合に備えて、付加的な対策が用意されている。 ・IDP と SP のサイトは、両方のサイトのクロックの設定が最大でも数分であることを確認するための合理的な努力をする必要がある。時刻同期のサービスの多くは、インターネット上、または特定のソースのいずれかで利用できる。 ・送信元サイトは、SAML アーティファクトが生成され、URL のライン上に配置された時と、アーティファクトを運ぶ<samlpRequest>のメッセージが送信先から受信された時の時間差を追跡するべきである。最大数分の時間制限が推奨される。アサーションは、この制限時間を超えて送信先サイトのクエリで要求されるべきである。送信元サイトは、送信先サイトにアサーションを提供してはならない。 ・送信元サイトは、対応する SAML アーティファクトが作成されるか、アーティファクトを運ぶ<samlp Request>のメッセージが送信先から受信された場合に、SSO アサーションを作成することができる。アサーションの有効期間は、	

脅　威	内　容	対　策	対応状況
		前者に合せて長めか、後者に合せて短めか、それぞれの場合で適切に設定するべきである。 ・SSO アサーションの NotBefore と NotOnOrAfter 属性の値は、IDP から SP のサイト間でアサーションが正常に交換できる最短の有効期間にすべきである。これは、数分というオーダが典型的である。これは、盗まれたアサーションが、わずかな時間の間しか正常に使用できないことを保証する。 ・SP サイトは、IDP サイトから取得したすべてのアサーションの有効期間をチェックし、期限切れのアサーションを拒絶しなければならない。SP サイトは、アサーションの IssueInstant または AuthnInstant 属性の値がアサーションを SP サイトで受信してから数分以内となるような SSO アサーションに対する有効性の厳格なテストを実装することを選ぶことができる。 ・SP サイトは、受信した認証ステートメントが利用者の IP アドレスを持った <samlSubjectLocality> の要素を含む場合、認証ステートメントに含まれている IP アドレスとブラウザの IP アドレ	

脅　威	内　容	対　策	対応状況
		スをチェックすることができる。	
6.4.2 SAML プロトコルメッセージ交換への攻撃	SP が使用する IDP からアサーションを取得するメッセージ交換は、アーティファクトやアサーションの盗難、リプレイ攻撃、メッセージの挿入・変更及び中間者攻撃などの様々な方法で攻撃できる。	双方向の認証、メッセージの完全性及び機密性の特徴を持ったSAMLプロトコルバインディングの利用要件は、これらの攻撃を防御する。	○ (Artifact バインディング)
6.4.3 悪意のある送信先サイト	SP は利用者からアーティファクトを取得するので、悪意のあるサイトがいくつかの新しい SP サイトで利用者を偽装することができる。新しい SP サイトは、IDP サイトからアサーションを取得し、悪意のあるサイトを利用者して信じる。	新しい SP サイトは、SAML アーティファクトに対応したSAMLアサーションを取得するためにIDPサイトで自分自身を認証する必要がある。これには 2 つの場合が考えられる。 1. 新しいSPサイトがIDPサイトと何の関係もない場合、認証することはできないし、このステップは失敗する。 2. 新しいSPサイトがIDPサイトと関係がある場合、IDPサイトは、アサーションがアーティファクトが最初に送信された以外の他のサイトによって要求されていることを決定する。このような場合、IDP サイトは新しい SP サイトにアサーションを提供してはならない。	○
6.4.4 偽造 SAML アーティファクト	悪意のある利用者はSAMLアーティファクトを偽造する可能性がある。	バインディング仕様は、現在も有効で使用できるアサーションのハンドルの値を推測あるいは構成することを実行不能にするようなSAMLアーティファクトの構	○

脅　威	内　容	対　策	対応状況
		築に関する推奨条件を提示している。悪意のある利用者は、(IDP サイトに存在するアサーションに対応する)有効な SAML アーティファクトの値を繰り返し推測することができる。しかし、値空間のサイズを考えると、このアクションは、おそらく非常に失敗の数が大きな試みが必要になる。IDP サイトは、存在しないアーティファクト対するクエリの繰返し試行によってアラームを発生させる対策を実装すべきである。	
6.4.5 ブラウザ状態の漏えい	SAML ブラウザ/アーティファクトプロファイルは、IDP のサイトから Web ブラウザに SAML アーティファクトの「ダウンロード」を含んでいる。この情報は、Web ブラウザの状態の一部として利用可能であり、通常は完全に保護されていない方法で利用者のシステムのストレージに継続的に格納されている。ここでの脅威は、アーティファクトが時間内に後の時点で「再利用」されることである。	SAML アーティファクトの「一回使用」の原則は、ブラウザから再利用できなくすることを保証する。アーティファクトと必須の SSO アサーションに関する短い寿命の推奨が、後で他のブラウザからアーティファクトの盗難と再利用を困難にする。	○ (アサーションの有効期間＝１分)
6.4.6 リプレイ攻撃	プロトコルメッセージの繰返しによるアーティファクトの再利用	アーティファクトの再利用のようなリプレイ攻撃は、アーティファクトを一時使用のアイテムとする要件で解決している。システムは、複数の要求が同じアーティファクトを参照する場合、侵入の試	○

脅　威	内　容	対　策	対応状況
		みである可能性が高いので追跡するべきである。	
6.5 URI バインデイング 6.5.1 置換	参照 URI の置換えによって、アサーションを別のものに置換。URI が受信者に明らかでない場合、完全性を検証するのは困難である。	これが懸念される場合、SSL/TLS のようなトランスポート層での完全性の保護が必要になる。	○
7.1.1 SSO プロファイル (1) 盗聴	すべての Web ブラウザで盗聴の可能性が存在する。	HTTP 伝送は、機密性が必要な場合、機密性を保証するトランスポート上で行う必要がある(セキュアに送信されていないアサーションは、それに関連付けられた要求と一緒に、悪意のある盗聴者が利用可能であることを念頭に置いて伝送する)。TLS/SSL 上の HTTP や IPsec は、この要件を満たす。	○
7.1.1 SSO プロファイル (2) 利用者認証情報の盗難	利用者が再利用可能な認証情報を漏らして送信元の認証を受ける場合には、例えば、パスワード形式では、認証情報の盗難で敵が対象を偽装できるようになる。	利用者のブラウザと送信元との間の接続は、この問題を回避するために、機密性の保護手段を実装しなければならない。さらに、ソースのサイトが認証情報を漏らす前に、利用者か送信先サイトのいずれかが真に期待と信頼のおける発行元のサイトであることを保証しなければならない。TLS 上の HTTP を使用すると、この問題に対処することができる。	○
7.1.1 SSO プロファイル	認証のアサーションが、アサーションのベアラの認証プロトコル識別子を含んでいる場合、敵がアーティファクトの盗難	以下の各方法は、この出来事の可能性を減少させる。 • 送信先サイトが利用者のブラウザとの	ー

脅　威	内　容	対　策	対応状況
(3) 無記名トークンの盗難	により対象を偽装できるようになる。	接続を保護する機密性対策を実装している。 ・利用者または送信先サイトが(アウトオブバンドで)送信元が利用者のブラウザとの接続を保護する機密性対策を実装していることを保証している。 ・送信先サイトが利用者のブラウザが利用者を直接認証した送信元によって直接リダイレクトされたことを確認する。 ・送信元サイトが同じアサーション ID に対応するアサーションに対する複数の要求に応答することを拒否する。 ・アサーションが特定のドメインを指定する AudienceRestrictionType 条件要素を含んでいる場合、送信先サイトでドメインのメンバーであることを確認する。 ・アサーション ID が通過する送信先サイトと送信元サイト間の接続が機密性を保護するように実装されている。 ・送信先サイトは、アサーション ID が通過する送信元サイトとの通信で、送信元サイトが真に期待と信頼のおける送信元サイトであることを検証しなければならない。	
7.1.1	ブラウザ、SAML アサーションの発行者、	トランスポートチャネルが保護されたデ	○

脅　威	内　容	対　策	対応状況
SSO プロファイル (6)メッセージの削除	およびSAMLアサーションの使用者の間のデータ交換のステップでのメッセージ削除は、データ交換が失敗する原因となる。これは、DOS攻撃をもたらすが、情報の漏えいが増えることはない。	ータの完全性を使用すると、仲介者が存在しない場合にメッセージ削除の脅威に対処できる。	
7.1.1 SSO プロファイル (7)メッセージの変更	ストリーム内のメッセージの変更の可能性がこのプロファイルの集合には存在する。いくつかの潜在的な望ましくない結果は次の通りである。 ・元の要求の変更がSAMLの発行者で拒絶されている結果となるか､要求されたものとは異なるリソースを対象としたアーティファクトの作成が起こされる。 ・アーティファクトの変更は、SAML の利用者にDOS攻撃を起こす可能性がある。 ・伝送中のアサーション自身の変更は、(署名がない場合は)悪い結果または(署名があるが消使用者がこれを拒否する場合は)DOS 攻撃を起こす可能性がある。	トラフィックは、メッセージ変更を避けるため、エンドポイント間でのメッセージの完全性を保証するシステムによって伝送する必要がある。 Webブラウザベースのプロファイルの場合、伝送中のメッセージの完全性を提供する推奨方法は、データの完全性チェックが提供された暗号化を使用したTLS/SSLによるHTTP伝送である。	○
7.1.1 SSO プロファイル (8)中間者	中間者攻撃は、特にこのプロファイルの集合に有害である。中間者攻撃では、要求が中継でき、返却アサーション(またはアーティファクト)を挿入でき、偽のものの返却が中継できる。その結果、本来の	このような脅威を防止するには、多くの対策が求められる。まず、強力な二者間の認証を提供するシステムの使用である。これにより、中間者がデータ交換に参加することがかなり困難になる。	○

脅　威	内　容	対　策	対応状況
	利用者は、中間者攻撃によって挿入されたリソースを取除いて、該当リソースにアクセスすることはできなくなる。	しかし、返されるアサーションまたはハンドラを挿入する(そしておそらく要求者に最終的な返答を変更する)ことを目的として、中間者が純粋に双方向のポート転送者として機能し、情報を盗聴される中間者攻撃の存在の可能性は依然としてある。機密性の高いシステムを置くことで盗聴を防ぐことができる。データの完全性の高いシステムを置くことでポートの転送中でのメッセージの改ざんを防止することができる。 TLS/SSL 層が(機密性やデータの完全性の提供に関して十分強力な)適切な暗号化を採用し、認証に 509v3 証明書を求める場合、このプロファイルの集合のため、強力な二者間のセッションの認証、機密性、およびデータの完全性のすべての要件は、TLS / SSL 上の HTTP を使用することで満たすことができる。	
7.1.1 SSO プロファイル (9)Impersonation without Reauthentication 再認証なし	不正な利用者が現在ログインしている正当な利用者に偽装する試みをして、保護されたリソースへのアクセスができるようになる。 利用者が IDP に正常にログインされると、それ以降はその利用者を再認証するために、他の SP からの<AuthnRequest>	IDP は、この脅威が問題になる実装では、利用者が最初に認証される前の<Response>を発行する前に、アクティブなセッションに関する状態情報を保持し、<AuthnRequest>とアクティブなセッションの間の対応を検証なければならない。IDP が発行したクッキーは、この	―

脅　威	内　容	対　策	対応状況
で偽装	メッセージは必要としない。しかし、IDPが利用者のIDを関連付けられられない、利用者の正当に認証されたIDPのセッションではないと判断できる場合は、利用者は認証を受ける必要がある。	検証プロセスのために使用されることがある。しかし、リバティがクッキーベースのアプローチを推奨しているものではない。	
7.1.2 拡張クライアントおよびプロキシのプロファイル (1)中間者	AuthnRequestとResponse SOAPメッセージをインターセプトして、その後続の利用者を偽装する。 不正なシステムエンティティは、拡張クライアントと正当なSPの間の自身が中間者として入込むことができる。エンティティは、拡張クライアントとのデータ交換においてSPとしての役割を務め、正当なSPとのデータ交換において拡張クライアントとしての役割を務める。中間者は、この方法でまず、SPのAuthnRequestをインターセプトし、拡張クライアントにAuthnRequestを転送する前に、PAOSヘッダブロックのresponseConsumerServiceURLに指定されたURLを置換える。中間者は、一般的に自分自身を指すURLの値を挿入する。もし、拡張クライアントが、その後でIDPから応答を受信して、中間者から受信したresponseConsumerServiceURLに応答を送信す	IDPは、拡張クライアントへ拡張クライアントが応答を送信しなければならないアドレスを指定する。PAOSヘッダのresponseConsumerServiceURLは、プロファイルで指定されているように、拡張クライアントからのエラー応答にだけ使用する。	○ (responseConsumerServiceURL)

脅　威	内　容	対　策	対応状況
	るならば、中間者は、正当な SP の利用者になりすますことができるようになる。		
7.1.2 拡張クライアントおよびプロキシのプロファイル (2) DOS	PAOS ヘッダブロックのサービス属性の値を未知の値に変更したり、ECP ヘッダブロックの ProviderID または IDPList を要求が失敗するように変更することによって、AuthnRequest の SOAP 要求が処理できないように変更する。	SOAP メッセージセキュリティや SSL / TLS を使用して、SOAP メッセージの完全性保護を提供する。	○
7.1.3 IDP 発見プロファイル	クッキーポイズニング攻撃は不正な IDP の発見がもたらされる。これは、クッキー内のパラメータが変更されている。	一般的なドメインを使用した、このメカニズムは、この脅威の可能性を制限する。	○ Cookie のドメインは制限あり
7.1.4 シングルログアウト	受動的な攻撃者が利用者の名前識別子を収集することができる。 受動的な攻撃者は、最初のリダイレクトのステップの間に<LogoutRequest>の情報を収集できる。これらのデータを公開することはプライバシに脅威を及ぼす。	すべてのデータ交換を SSL や TLS などのセキュリティで保護されたトランスポート上で実施するべきである。	－ (今回はマルチサイトは対象外となるため、シングル Logout は対象外とする)
	署名なし<LogoutRequest>メッセージは、不正なシステムエンティティによって挿入することができる。これにより、利用者へのサービスが遮断される。 名前 ID が推測または派生させることができると仮定すると、利用者エージェントがでっち上げた<LogoutRequest>メッセージの配信を指示できることが考えられる。	<LogoutRequest>メッセージに署名する。IDP は、署名付き要求がない場合でも対象の ID を確認することができる。	－ (今回はマルチサイトは対象外となるため、シングル Logout は対象外とする)

脅　威	内　容	対　策	対応状況
7.2 名称識別子管理プロファイル	情報の紐付やプライバシを傷つける身元情報の不正な公開をシステムエンティティに許可する。	IDP は、同じ対象に対して SP 毎に別の識別子を使用するように注意する必要がある。IDP は、その後の通信で不明な識別子が使用できるように、SP に返す名前識別子を暗号化する必要がある。	－

表 3.1.1-2　SSL/TLS の脆弱性とその対策に対する対応

脅　威	内　　容	対　　策	対応状況
SSL 適用の適切さ	データ保護が必要な場合に適切に SSL が使われていない場合、通信の安全性は保障されない。	・SSL が必要なときに正しく使われているかどうかは、利用者自身が判断する。 ・World Wide Web では、ハイパーリンクによるページ遷移を繰り返して処理を行うため、どの通信で SSL/TLS が使用されているか把握する。	SAML 認証ではすべて SSL での通信を行うこととなっている。
下位層への攻撃に対する脆弱性	ネットワーク層以下のレイヤにおいて適切な対策を取っていない場合、これらの層で ARP 詐称やセッション乗っ取り、中間者攻撃が行われた場合、メッセージ挿入、メッセージ改ざん、中間者攻撃等の攻撃を受ける場合がある。	・接続サイトが「医療情報システムの安全管理に関するガイドライン」に準じてリスク分析を行って、セキュリティ対策が施してあることを確認する。	本仕様の対象外の項目である。

推奨できないアルゴリズムの採用	仕様として許容はされているが推奨できないアルゴリズムでクライアントがネゴシエーションを行ってきた。通信の安全性が保証できない。	・ダイアログメッセージなどを使って利用者に警告する。 ・推奨できないアルゴリズムでの接続は拒否する。 -SSLv2 以前の接続要求は拒否する。 -高いセキュリティが要求される実装では 40 ビットの鍵を認めない。 -匿名の Diffie-Hellman はなりすまし攻撃を防ぐことができない。 -アプリケーションで最小と最大の鍵サイズを強制する。例えば、512 ビットの RSA 鍵または署名を含む証明書チェーンは高セキュリティアプリケーションに対して適切ではない。	医療認証基盤システム側では以下のネゴシエーションを許可している。 SSL Version : SSL 3.0/TLS1.0 暗号： 3DES(168bit)、AES(128bit/256 bit)、Camellia(128bit /256bit) MAC : SHA-1
なりすまし	「認証局は自身の秘密鍵を厳重に秘匿し、また証明書の発行にあたっては正当なサーバ管理者かどうか確認する」ことが保証されていない認証局のルート証明書を組込む。認証局が安全でも、入手したルート証明書が本当に意図する認証局のものかどうか判断することが難しい。	・認証局は自身の秘密鍵を厳重に秘匿し、また証明書の発行にあたっては正当なサーバ管理者かどうか確認する。 ・証明書失効メッセージをサポートする。 ・利用者が証明書及びルート CA に関する情報を確認できるようにする。	VeriSign 社のサービスを利用してサーバ証明書を発行している。

サーバ名の詐称	サーバ A の管理権限を持たない者がサーバ B として正当な証明書を取得し、その証明書を使ってサーバ A を名乗る。	・SSL で認証を行う場合に、認証局の署名に加えて、サーバ証明書で発行先サーバのホスト名を確認する。この検証は、システムに指示された送信先のホスト名と実際に接続した先のホスト名が一致することを検証する。 ・利用者が意図する送信先と一致することを検証するため、以下の 2 つの条件を整える。 1.利用者は、意図する送信先の正しいホスト名を知っている。 2.利用者は、現在システムに指示されている送信先が、自分の知っている正しいホスト名と一致していることを確認できる。	証明書（秘密鍵）の管理を医療認証基盤システムのサーバ内で管理。 auth.pki.med.or.jp saml.pki.med.or.jp はグローバルアドレスとして DNS に登録されている。
Debian の脆弱性	OpenSSL ライブラリのパッケージに不適切なパッチを導入した場合、鍵生成に適切な乱数が使わず、65536(=216)通りの予測可能な鍵が生成される。この影響は、OpenSSL で作られた鍵全て、SSH 鍵、OpenVPN 鍵、DNSSEC 鍵、X.509 証明書を生成する鍵データ、SSL/TLS コネクションのセッション鍵等が受ける。生成された鍵に問題があるため、Debian GNU/Linux で生成した鍵を Microsoft Windows のような非 UNIX システムに導入する場合も影響を受ける。	・以下の OpenSSL パッケージを使用する場合、Debian の報告の他、JPCERT/CC の勧告等に準拠してシステムを提供する。 Debian sarge より後の Debian, Damn Small Linux, KNOPPIX, Linspire, Progeny Debian, sidux, Ubuntu, UserLinux, Xandros	Redhat Enterprise Server を利用。 また、openssl については 1.0.0.d をダウンロードして導入している。

再ネゴシエーション脆弱性	SSL 3.0 以降の再ネゴシエーション機能を利用して、クライアントからのリクエストの先頭に中間者が任意のデータを挿入できる。プロトコル自体の脆弱性であり、すべての実装が影響を受ける。この脆弱性は、サーバが対応しない限り、クライアントは再ネゴシエーションが発生したことを検出できない。クライアント単体で対応することはできない。	・サーバにおいて再ネゴシエーションを禁止する。 ・サーバが再ネゴシエーション手順を RFC 5746 の TLS Extension を使った手順にする。	・openssl1.0.0d を適用（RFC 5746 対応済み）
バージョンロールバック攻撃	なりすましによってセッションを脆弱性のある過去のバージョンのアルゴリズムに変更して、様々な攻撃をする。	・TLS をサポートするサーバは、ENCRYPTED-KEY-DATA フィールドを復号した後、それら 8 つのパディングバイトが 0x03 であればエラーとする。 ・40 ビットの暗号鍵を使用しない。	・openssl1.0.0d を適用(JVN#23632449 対応済み) ・SSLv2 での接続を許可していない
ハンドシェイクプロトコルに対する攻撃	ハンドシェイクプロトコルに対する攻撃を検知してセッションへの不要な攻撃を回避する。	・セションが危険に晒されている、または証明書の有効期間が切れたか取り消されている場合は、完全なハンドシェイクを実施する。 ・安全でない環境で実行されるアプリケーションは、セション ID を静的な記憶装置に書き込まないようにする。	・openssl1.0.0d を適用(JVNVU#520586 対応済み)

(f)　アサーションの構造

SAML の認証に用いる HPKI の hcRole は標準化の投票にかけられている段階であり、標準化されない場合も想定される。このため、開発した成果物は、このような標準化の動向に依らず、継承性や機能拡張のあるものであることが望ましい。このため、アサーションの構造が hcRole やその他の標準化動向と併存可能なものであり、標準化の動向と無関係に継承性を持って使えることを示す。

本事業では、認証アサーションの”AttributeStatement”に属性情報を指定する方式とした。” AttributeStatement”を以下のように使用する。

Name=”hcRole”
saml:AttributeValue=”MedicalDoctor”

<Attribute Name=”hcRole”>
<saml:AttributeValue>MedicalDoctor</saml:AttributeValue>
</Attribute>

認証アサーションの属性と要素の構成を表 3.1.1-3 に示す。属性ステートメントの属性と要素の構成を表 3.1.1-4 に示す。

表 3.1.1-3　認証アサーションの属性と要素の構成

パラメータ	要否	値	内　　容
“Assertion” Attribute			
Version	Required	"2.0"	アサーションのバージョンを指定する。
ID	Required	xs:ID	400 ビット以内の桁でアサーションの ID を指定する。
IssueInstant	Required	UTC time	アサーションの発行時刻を指定する。
“Assertion” Elements			
saml:Issuer	Required	URI	アサーションのクレームを作成した SAML オーソリティの URI を指定する。
ds:Signature	Optional		アサーションの真正性を守り、発行者を認証する XML 署名を指定する。
Saml:Subject	Optional		拡張スキーマで定義される Subject の方向を指定する。
Saml:Conditions	Optional		アサーションの有効性を評価する時に考慮すべき条件を指定する。
Saml:Advice	Optional		アサーションの付加情報を指定する。
saml:Statement	Optional		任意の情報を指定する。
saml:AuthnStatement	Optional		認証情報を指定する。
saml:AuthzStatement	Optional		認可情報を指定する。
Saml:AttributeStatement	Optional		属性情報を指定する。

表 3.1.1-4　属性ステートメントの属性と要素の構成

パラメータ	要否	値	内　　容
“Attribute” Attribute			
Name	Required		属性の名称を指定する。
NameFormat	Optional	URI	属性の名称を解決するための参照 URI を指定する。NameFormat の値が指定されていない場合は、urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified を参照する。
FriendlyName	Optional		実際の名称が OID や UUID のような複雑あるいは不透明な場合に可読な属性名を指定する。この属性の値は、SAML 属性を識別するために基本的に使用しない。
“Attribute” Element			
saml:AttributeValue	Any Number		属性の値を指定する。属性が複数の離散的な値を持つ場合、それぞれの別の <AttributeValue>要素に値を設定する。<AttributeValue>要素がない <Attribute>要素は無視する。複数の値が xsi:type の場合、値は同一のデータ型にする必要がある。 属性は、NameFormat と XML 属性の Name の組合せによって識別または名称付けする。NameFormat には、いくつかのシナリオの用法に関する相互運用性を改善するために設計された属性のプロファイルが含まれている。どちらかが一意であると仮定できるが、組合せて曖昧さを排除しなければならない。

本件において考慮すべき外部の動向や場合としては、以下に示す 3 つの場合が考えられる。

- hcRole の標準化動向
- 属性やポリシーを扱う XACML 等の標準化動向
- 個人が複数の資格を持つ場合

本実証において、これら 3 つの場合の状況に関わらず、継承性を持って使えることを示す。

① hcRole の標準化動向

hcRole の標準化が現在進められているが、hcRole の標準化の如何に関わらず、使用できる構造になっているか考慮する必要がある。

hcRole は、HPKI の”SubjectDirectoryAttributes”として規定されている。この” SubjectDirectoryAttributes”は、ヨーロッパ各国では空欄となっている。hcRole に対応する本人の属性は、ID 番号に対応させて別のシステムで紐付けられている。

SAML では、認証や属性情報の提示を行うシステムは「認証オーソリティ」や「属性オーソリティ」と呼ばれる。認可決定及びアクセス制御を行うシステムは、それぞれ「ポリシー決定点」（PDP）、「ポリシー実行点」（PEP）と呼ばれる。SAML は、これらのシステム間やクライアントとの間のデータ交換方法と認証･属性･認可情報の記述フォーマット（アサーション）を規定する。

SAML をモデルとすると、この属性が紐付けられている別のシステムは、「属性オーソリティ」または「ポリシー決定点」（PDP）と考えることができる。この場合、本事業で規定した認証オーソリティから返却される「認証アサーション」ではなく、属性アサーションまたは認可アサーションによって hcRole などの属性のデータ交換を行うと考えられる。

HPKI のような公開鍵証明書に指定された属性情報を送信する場合、「属性オーソリティ」または「ポリシー決定点」（PDP）などの別システムで属性が管理された場合と異なり、本事業のように「認証オーソリティ」で認証情報として情報が取得できるため、認証アサーションで一緒にデータ交換した方が効率的と考えられる。また、これを「属性アサーション」として特に分けてデータ交換する必然性もない。

したがって、公開鍵証明書に記載された情報を属性情報として送信する場合、本事業で規定した方法で Attribute の属性として指定

する”Name”を必要に応じて規定することによって拡張すれば十分に対応できると考えられる。

② 属性やポリシーを扱う XACML の標準化動向

SAML の機能拡張に使われる併用規則として、属性やポリシーを扱う XACML のようなものがある。これらの関係する言語の標準化の動向に関わらず、使用できる構造になっているか考慮する必要がある。

XACML は、SAML 同様、XACML 処理系への認可要求と結果応答を XACML コンテキストの形でデータ交換する。XACML コンテキストは、要求と応答のフォーマットのみを規定しているため、任意の実装にマッピングできる。このため、SAML で PDP と PEP の間でデータ交換する場合、XSLT などを使って XACML コンテキストと SAML 認可プロトコルの間の変換を行うことができる。

本実証では、PDP と PEP の二つの機能要素は SP の内部にあるモデルに基づいて構成している。この場合、XACML の適用箇所は、SP 内の機能要素間の内部での引継パラメータに相当する部分に当たる。このため、XACML の仕様化する部分と本実証での開発機能が重複することがない。したがって、本事業の仕様は、XACML での属性やポリシー等の標準化に関わらず、継承できると考えられる。

③ 個人が複数の資格を持つ場合の対応

hcRole では、複数の資格を持った人に対して複数の資格を持っていることが表現できる。今後、医師以外に対象を拡げる場合に複数の資格を持つことを表現できる構造になっているか考慮する必要がある。

“AttributeStatement”は、任意の回数組み合わせて使用できる。このため、複数の資格を持った人は、アサーションの中でこの“AttributeStatement”を所持している資格の数だけ指定することによって対応できる。

(g) SAML ユースケースについての検討

医療機関連携や医療情報の共有に関するシステムにおいて、医療認証基盤のような共同利用型の認証センターが有効そうな事例をユースケースとして検討する。

① 参照型

医療機関の医師が他の医療機関の情報を閲覧・参照する参照型の「シームレスな地域連携医療」がある。この事例としては、一つは、高齢者が複数疾患に罹っている場合に、それぞれの疾患別に専門の病院に罹っている場合も多い。このような場合、専門医が一つの医療圏内に必ずしもいるとは限らない。特に過疎が問題となっている地域ほどこの傾向があると考えられる。このような専門医が広域でシェアされる場合に有効と考えられる。

もう一つとして、居住している二次医療圏から外への医療圏に勤務、旅行や救急などの理由で一時的に患者が異動している時に罹患した場合に発生する。このような場合、医師は、元の二次医療圏のシームレスな地域連携医療が保持する情報を参考にするために参照する。しかし、多くの場合は元の二次医療圏では医師がシステムに登録されていないと考えられる。したがって、このような場合の連携には第三者認証を共同で利用することが有効と考えられる。

② 受領型（シームレスな地域連携医療）

診療情報提供書、画像検査結果等の伝送等の情報をデータ交換する受領型の「シームレスな地域連携医療」がある。この事例としては、一つは、患者が患者の転居や他の医療機関の紹介等によって他の医療圏に異動した場合に診療サマリとして診療情報提供書、画像検査結果等を受渡す場合がある。このような場合、異動先の医師が登録管理されているとは考えられない異動元の医療圏の情報をタイムリーに得るために、三次医療圏以上の広域な資格確認ができると有効である。

もう一つとして、疫学研究、症例研究等の二次利用に関するアクセスが考えられる。疫学研究、症例研究のために、医師、薬剤師、歯科医師等が電子カルテや医療情報データベースまたはレセプト情報のデータベースにアクセスする場合、公益性があり、広域でのアクセスが考えられるため、アクセスする人の資格や本人確認を厳格に行う必要がある。このような場合に、第三者認証による客観的な

認証に関する証明はコンプライアンスの点で有効である。

③ 患者管理型

患者が「どこでも My 病院」に登録した情報や処方箋などを医師や薬剤師に渡す場合がある。この事例では、「どこでも My 病院」のシステムは、「患者が情報を渡したい相手」の本人性や医師や薬剤師としての資格の有無を確認する必要があるが、これを適正に行うには「どこでも My 病院」システムに必要が出た都度、或いはアクセスが想定される地域のすべての医師や薬剤師に関わる認証情報の登録・管理をすることが求められる。

このような認証情報の登録・管理を地域毎に行う場合、医師や薬剤師が複数の地域で登録・管理する必要があり、各地域で資格確認を行うことも含めて認証に関わる運用コストがかなり増大すると考えられる。このため、第三者が医師や薬剤師のような国家資格のある人間の本人性を含めて検証してもらえると、システムの運用に関わるコストを大幅に削減することができる。また、患者が医師や薬剤師に安心して自分の情報を預けるために有効である。

3.1.2. 実現した効果

本事業によって得られた成果をまとめると次の 3 点である。

（1） 高い信頼性や安全性を持った医療認証基盤の提供

第 3.1.3 節次頁以降に示す目標管理、システム管理及び品質管理指標を設定し、定量的に目標値をクリアした信頼性や安全性の高いシステムを提供することができた。

（2） 医療分野の共通基盤となる共通モジュールの提供

共通モジュールは、各サイトのシステム形態に合わせてプロキシ型と API 型の 2 つのタイプから選択して実装できる「SAML 連携モジュール」を提供することができた。

（3） マルチベンダ環境での相互運用性の確保

異なる実装環境のシステムと相互接続をするための仕様書として、「SAML 実装仕様書」を提供することができた。

本事業では、以上のような技術的な実証成果を踏まえて、日本医師会が公益法人として事業提供することによって、医療圏に依らず、全国規模で地域連携医療や救急医療で医師が医療情報を診療に有効に利用できることが実証できた。これにより、過去の治療歴、手術歴、患者サマリなどが格納された SS-MIX 標準化ストレージが各地にできることによって、患者の特徴や正確な医療・介護情報に基づいて、医師が正確な判断ができる診療環境を構築できる可能性を示すことができた。このような環境が整えられることにより、「どこでも、どの医師でも、目の前の患者の状況に合せたテーラーメイドの医療ができ、医療の品質をさらに向上させる」ことが期待できる。

3.1.3. 成果指標の達成状況

医療認証基盤整備事業について、設定した評価指標に基づいて事業の実施内容及び開発した連携モジュールの完成度を評価する。本件について、大別すると、下記の二つの項目について評価する。

① 目標管理に関する評価
② システム管理及び品質管理に関する評価

（1） 目標管理に関する評価

(a) 評価項目

目標管理に関する評価項目を表 3.1.2-1 に示す。

表 3.1.2-1 目標管理の達成度

分類	評価指標	評価項目
目標管理	標準化	実装する機能に関する SAML プロトコルの機能仕様書ができている。
		SAML プロトコルの実装規約が曖昧さを排除して仕様書化されている。
		相互接続試験ができる試験仕様書が作成できている。
		標準化資料の多様な解釈ができる部分を明確に規定して相互運用性が確保できる。
		オープンソース等の他のベンダが開発の参考になる有用な情報が提供されている。
	継承性	実装仕様書の内容や作成資料を外部の標準化団体、利用者に広く公開している。
		実装仕様書の内容を外部の標準化団体、利用者で普遍的なものにする作業をしている。
		実装において機能仕様を明確にした部分を標準化団体に標準化するように提案している。
		関係省庁の間で開発した技術内容を共有して再利用を可能にしている。
		相当機能の開発を支援する開発コード、サンプルソース等が十分に提供されている。
		取扱説明書等の導入に関わる資料が用意されている。
	性能・安全性	個人情報保護に関する当該分野の法制度、ガイドラインを踏まえた検討がされている。
		法制度、ガイドラインを踏まえたシステムのセキュリティが評価されている。
		レスポンスタイムが問題ない範囲の設計方式となっている。
		ターンアラウンドタイムが問題ない範囲の設計方式となっている。
	経済性	実装仕様書で設計・試験工数を抑制できる。
		製造した共通モジュールでシステムの認証に関わる設計・構築の工数を抑制できる。
		製造した共通モジュールのシステム要件が導入し易いものになっている。
		製造した共通モジュールの導入によって運用維持コストを抑制できる。

(b)　評価方法

目標管理の評価方法は、技術運用連絡会議のメンバに評価項目を評価シートに沿って 5 段階評価で評価してもらう。各評価項目について、評点が平均で目標値の 4 以上場合に評価項目に関する目標が達成できたと判定する。

評価シートで聴いた各項目の評価内容を以下に示す。

① 標準化

(i) 実装する機能に関する SAML プロトコルの機能仕様書ができている。

5. 機能仕様書として曖昧さが排除された十分な内容である。
4. 機能仕様書として十分な内容である。
3. 機能仕様書が作成されている。
2. 機能仕様書に類するものがある。
1. 機能仕様書が作成されていない。

(ii)SAML プロトコルの実装規約が曖昧さを排除して仕様書化されている。

5. 実装規約として曖昧さが排除された十分な内容である。
4. 実装規約として十分な内容である。
3. 実装規約が作成されている。
2. 実装規約に類するものがある。
1. 実装規約が作成されていない。

(iii)相互接続試験ができる試験仕様書が作成できている。

5. 試験仕様書として曖昧さが排除された十分な内容である。
4. 試験仕様書として十分な内容である。
3. 試験仕様書が作成されている。
2. 試験仕様書に類するものがある。
1. 試験仕様書が作成されていない。

(iv) 標準化資料の多様な解釈ができる部分を明確に規定して相互運用性が確保できる。

5. 実装仕様書として曖昧さが排除された十分な内容である。
4. 実装仕様書として十分な内容である。

3. 実装仕様書が作成されている。
2. 実装仕様書に類するものがある。
1. 実装仕様書が作成されていない。

(v) オープンソース等の他のベンダが開発の参考になる有用な情報が提供されている。

5. 新しく検討された内容が曖昧さを排除した公開できる文書として提供されている。
4. 新しく検討された内容が公開できる文書として提供されている。
3. 新しく検討された内容が提供されている。
2. 新しく検討された内容が提供されていない。
1. 新しく検討された内容がない。

② 継承性

(i) 実装仕様書の内容や作成資料を外部の標準化団体、利用者に広く公開している。

5. 実装仕様書を広報によって働きかけて外部に積極的に公開している。
4. 実装仕様書を個別に働きかけて外部に公開している。
3. 実装仕様書を外部に公開している。
2. 実装仕様書を外部に公開する努力をしている。
1. 実装仕様書が外部に公開されていない。

(ii) 実装仕様書の内容を外部の標準化団体、利用者で普遍的なものにする作業をしている。

5. 関係者を集めた会議で実装仕様書の有用性が認められている。
4. 関係者を集めた会議で実装仕様書を有用にする努力をしている。
3. 関係者を集めた会議で実装仕様書について評価している。
2. 関係者に個別訪問している。
1. 何もしていない。

(iii) 実装において機能仕様を明確にした部分を標準化団体に標準化するように提案している。

5. 標準化団体に提案している。
4. 標準化団体に提案できる内容になっている。

3. 標準化に寄与できる内容になっている。
2. 標準化に寄与できる内容にする努力をしている。
1. 標準化に寄与できる内容になっていない。

(iv) 関係省庁の間で開発した技術内容を共有して再利用を可能にしている。

5. 実装仕様書として曖昧さが排除された関係省庁で利用できる十分な内容である。
4. 実装仕様書として関係省庁で利用できる十分な内容である。
3. 実装仕様書として関係省庁が利用できる内容である。
2. 実装仕様書として関係省庁が参考にできる内容である。
1. 実装仕様書として関係省庁が参考にできない内容である。

(v) 相当機能の開発を支援する開発コード、サンプルソース等が十分に提供されている。

5. 開発を支援する開発コード、サンプルソース等が十分に提供されている。
4. 開発を支援する開発コード、サンプルソース等が提供されている。
3. 開発を支援する開発コード、サンプルソース等が断片的に提供されている。
2. 開発を支援する開発コード、サンプルソース等に類するものがある。
1. 開発を支援する開発コード、サンプルソース等が作成されていない。

(vi) 取扱説明書等の導入に関わる資料が用意されている。

5. 取扱説明書等の導入に関わる資料として曖昧さが排除された十分な内容である。
4. 取扱説明書等の導入に関わる資料として十分な内容である。
3. 取扱説明書等の導入に関わる資料が作成されている。
2. 取扱説明書等の導入に関わる資料に類するものがある。
1. 取扱説明書等の導入に関わる資料が作成されていない。

③ 性能・安全性

(i) 個人情報保護に関する当該分野の法制度、ガイドラインを踏まえた検討がされている。

5. 「医療情報システムの安全管理に関するガイドライン」の要件に準拠して実装されている。
4. 「医療情報システムの安全管理に関するガイドライン」の要件に準拠して設計されている。
3. 「医療情報システムの安全管理に関するガイドライン」を踏まえて技術検討されている。
2. 「医療情報システムの安全管理に関するガイドライン」の要件に準拠して運用されている。
1. 一般的な技術に基づいてセキュリティが検討されている。

(ii)法制度、ガイドラインを踏まえたシステムのセキュリティが評価されている。

5. 法制度、ガイドラインを踏まえたチェックシートでセキュリティを十分なものにしている。
4. 法制度、ガイドラインを踏まえたチェックシートでのセキュリティ評価に基づいて改善している。
3. 法制度、ガイドラインを踏まえたチェックシートでセキュリティを評価している。
2. 法制度、ガイドラインを踏まえてセキュリティを自己評価している。
1. 法制度、ガイドラインを踏まえたシステムのセキュリティが評価されていない。

(iii)レスポンスタイム(処理要求送信から処理要求受信まで)が問題ない範囲の設計方式となっている。

5. レスポンスタイムとして十分な性能である。
4. レスポンスタイムとして問題ない範囲の性能である。
3. レスポンスタイムとして許容できる範囲の性能である。
2. レスポンスタイムとしてやや許容できない性能である。
1 レスポンスタイムとして許容できない性能である。

(iv) ターンアラウンドタイム(入力開始から出力終了まで)が問題ない範囲の設計方式となっている。

5. ターンアラウンドタイムとして十分な性能である。
4. ターンアラウンドタイムとして問題ない範囲の性能である。
3. ターンアラウンドタイムとして許容できる範囲の性能である。
2. ターンアラウンドタイムとしてやや許容できない性能である。
1. ターンアラウンドタイムとして許容できない性能である。

④ 経済性

(i) 実装仕様書で設計・試験工数を適切なものにできる。

5. 認証に関する機能設計・詳細設計・試験の工程を抑制できる。
4. 認証に関する機能設計・詳細設計の工程を抑制できる。
3. 認証に関する機能設計の工程を抑制できる。
2. 認証に関する機能設計の参考になる。
1. 機能設計に役立つものになっていない。

(ii)製造した共通モジュールでシステムの認証に関わる設計・構築の工数を抑制できる。

5. 共通モジュールで医師の認証に関わるシステム設計・構築が不要になる。
4. 共通モジュールを医師の認証に関わるシステムの設計・構築が簡単にできる。
3. 共通モジュールで医師の認証に関わるシステムの設計・構築ができる。
2. 共通モジュールでも医師の認証に関わるシステムの設計・構築は難しい。
1. 医師の認証に関わるシステムは個別に設計・構築した方がよい。

(iii)製造した共通モジュールのシステム要件が導入し易いものになっている。

5. 共通モジュールのシステム要件が導入し易いものになっている。
4. 共通モジュールのシステム要件での導入はハードルが高くない。
3. 共通モジュールのシステム要件での導入はハードルが高いが導入はできる。

2. 共通モジュールのシステム要件での導入はハードルが高いが導入の検討はできる。
1. 共通モジュールのシステム要件では導入できない。

(iv)製造した共通モジュールの導入によって運用維持コストを抑制できる。

5. 共通モジュールの導入によって地域外の医師の認証及び登録管理が不要になる。
4. 共通モジュールの導入によって医師の認証及び登録管理が不要になる。
3. 共通モジュールの導入によって医師の登録管理が不要になる。
2. 共通モジュールの導入によって医師の登録管理が一部不要になる。
1. 共通モジュールの導入によって医師の登録管理が並行して必要である。

(c)　評価結果

評価シートに基づいて、技術運用連絡会議のメンバ 17 名に評価していただいた。評点は、すべての項目について 4 以上の評価であった。このため、目標管理に関しては、すべての評価項目について目標が十分に達成できたと考える。

各評価項目の評価結果を表 3.1.2-2 に示す。

表 3.1.2-2　目標管理の達成度

分類	評価指標	評価項目	目標値	評点
目標管理	標準化	実装する機能に関する SAML プロトコルの機能仕様書ができている。	4 以上	4.6
		SAMLプロトコルの実装規約が曖昧さを排除して仕様書化されている。	4 以上	4.4
		相互接続試験ができる試験仕様書が作成できている。	4 以上	4
		標準化資料の多様な解釈ができる部分を明確に規定して相互運用性が確保できる。	4 以上	4.6
		オープンソース等の他のベンダが開発の参考になる有用な情報が提供されている。	4 以上	4.2
	継承性	実装仕様書の内容や作成資料を外部の標準化団体、利用者に広く公開している。	4 以上	4
		実装仕様書の内容を外部の標準化団体、利用者で普遍的なものにする作業をしている。	4 以上	4.2
		実装において機能仕様を明確にした部分を標準化団体に標準化するように提案している。	4 以上	4
		関係省庁の間で開発した技術内容を共有して再利用を可能にしている。	4 以上	4.4
		相当機能の開発を支援する開発コード、サンプルソース等が十分に提供されている。	4 以上	4.4
		取扱説明書等の導入に関わる資料が用意されている。	4 以上	4.4
	性能・安全性	個人情報保護に関する当該分野の法制度、ガイドラインを踏まえた検討がされている。	4 以上	4.4
		法制度、ガイドラインを踏まえたシステムのセキュリティが評価されている。	4 以上	4.6
		レスポンスタイムが問題ない範囲の設計方式となっている。	4 以上	5
		ターンアラウンドタイムが問題ない範囲の設計方式となっている。	4 以上	5
	経済性	実装仕様書で設計・試験工数を抑制できる。	4 以上	4.4
		製造した共通モジュールでシステムの認証に関わる設計・構築の工数を抑制できる。	4 以上	4.2
		製造した共通モジュールのシステム要件が導入し易いものになっている。	4 以上	4.6
		製造した共通モジュールの導入によって運用維持コストを抑制できる。	4 以上	4.2

（2） システム管理及び品質管理に関する評価

(a) 評価項目

システム管理及び品質管理に関する評価項目を表 3.1.2-3 に示す。

表 3.1.2-3 システム管理及び品質管理に関する評価項目

分類	評価指標	評価項目
システム管理	設計	設計レビューでの問題点の指摘がシステムの設計規模に見合っている。
		設計が計画通り一定の品質で進捗しているので設計レビューの回数が増加しない。
		設計が計画通り一定の品質で進捗しているので計画した時間内で設計レビューができる。
		設計・開発工程全体の中で設計レビューが効果的に実施されている。
		設計レビューが効率的に実施されている。
	試験	機能項目、設定データ等の試験項目の設定が開発規模に対して妥当なものになっている。
		機能項目、設定データ等の試験項目が品質からして網羅性があるものになっている。
		机上デバグにおける摘出バクが一定の基準以下で品質が安定している。
		工程毎バグ摘出件数が一定の基準以下で品質が安定している。
	納期	工程毎の納期が達成できている。
		納期毎の遅延が抑えられている。
品管質理	品質	リリース後に発見されたバグの件数が想定される範囲内にある。
	コスト	工程毎の開発要員及び工数が計画通りである。

(b) 評価方法

以下の評価方法に沿って開発各社が開発中で取得したデータに基づいて判定する。

① システム管理

(i) 設計

(ｱ) 設計レビューでの問題点の指摘がシステムの設計規模に見合っている。

評価式=指摘件数/レビュー対象規模(機能項目数)×100

目標値=10 以下

(ｲ) 設計が計画通り一定の品質で進捗しているので設計レビューの回数が増加しない。

評価式=実施件数/レビュー実施予定数×100

目標値=100 以下

(ｳ) 設計が計画通り一定の品質で進捗しているので計画した時間内で設計レビューができる。

評価式=レビュー対象規模/レビュー時間

目標値=1 分/項目以下

(ｴ) 設計・開発工程全体の中で設計レビューが効果的に実施されている。

評価式=レビュー時指摘バグ数/(レビュー時指摘バグ数+試験時指摘バグ数)×100

目標値=50 以上

(ｵ) 設計レビューが効率的に実施されている。

評価式=指摘件数/レビューにかけた工数(hour)×100

目標値=50 以上

(ii)試験

(ｱ) 機能項目、設定データ等の試験項目の設定が開発規模に対して妥当なものになっている。

評価式=試験項目件数/機能項目数×100

目標値=100 以上

(ｲ) 機能項目、設定データ等の試験項目が品質からして網羅性があるものになっている。
評価式=試験実施分岐数/全分岐数×100
目標値=10 以上

(ｳ) 机上デバグにおける摘出バクが一定の基準以下で品質が安定している。
評価式=机上デバグ摘出バグ件数/実ソースコード規模に応じた想定バグ件数×100
目標値=100 以下

(ｴ) 工程毎バグ摘出件数が一定の基準以下で品質が安定している。
評価式=試験時指摘バグ数/実ソースコード規模に応じた工程別の想定バグ件数×100
目標値=100 以下

(iii)納期
(ｱ) 工程毎の納期が達成できている。
評価式=工程毎の達成件数/全完了件数×100
目標値=95 以上

(ｲ) 納期毎の遅延が抑えられている。
評価式=Σ(契約納入日-納入日)/Σ工期日数×100
目標値=5 以下

② 品質管理
(i) 品質
(ｱ) リリース後に発見されたバグの件数が想定される範囲内にある。
評価式=出荷後一定期間内の障害件数/(レビュー時指摘バグ数+試験時指摘バグ数)×100
目標値=1 以下

(ii)コスト

(ｱ) 工程毎の開発要員及び工数が計画通りである。

評価式=(開発要員×工数)/(開発要員の計画値×工数の計画値)×100

目標値=100 以下

(c)　評価結果

評点は、すべての項目について目標値を達成していた。このため、システム管理及び品質管理に関しては、測定可能なすべての評価項目について目標が十分に達成できたと考える。

各評価項目の評価結果を表 3.1.2-4 に示す。

図 3.1.2-4 システム管理及び品質管理の達成度（日本電気）

分類	評価指標	評価項目	目標値	評点
システム管理	設計	設計レビューでの問題点の指摘がシステムの設計規模に見合っている。	10 以下	2.80
		設計が計画通り一定の品質で進捗しているので設計レビューの回数が増加しない。	100 以下	77.8
		設計が計画通り一定の品質で進捗しているので計画した時間内で設計レビューができる。	1 分/項目以下	0.005
		設計・開発工程全体の中で設計レビューが効果的に実施されている。	50 以上	59.1
		設計レビューが効率的に実施されている。	50 以上	185
	試験	機能項目、設定データ等の試験項目の設定が開発規模に対して妥当なものになっている。	100 以上	1873
		機能項目、設定データ等の試験項目が品質からして網羅性があるものになっている。	10 以上	100
		机上デバグにおける摘出バクが一定の基準以下で品質が安定している。	100 以下	100
		工程毎バグ摘出件数が一定の基準以下で品質が安定している。	100 以下	30.2
	納期	工程毎の納期が達成できている。	95 以上	100
		納期毎の遅延が抑えられている。	5 以下	0
品質管理	品質	リリース後に発見されたバグの件数が想定される範囲内にある。	1 以下	0
	コスト	工程毎の開発要員及び工数が計画通りである。	100 以下	100

図 3.1.2-4 システム管理及び品質管理の達成度（三菱電機インフォメーションシステムズ）

分類	評価指標	評価項目	目標値	評点
システム管理	設計	設計レビューでの問題点の指摘がシステムの設計規模に見合っている。	10 以下	6.25
		設計が計画通り一定の品質で進捗しているので設計レビューの回数が増加しない。	100 以下	100
		設計が計画通り一定の品質で進捗しているので計画した時間内で設計レビューができる。	1 分/項目以下	-
		設計・開発工程全体の中で設計レビューが効果的に実施されている。	50 以上	-
		設計レビューが効率的に実施されている。	50 以上	-
	試験	機能項目、設定データ等の試験項目の設定が開発規模に対して妥当なものになっている。	100 以上	583.3
		機能項目、設定データ等の試験項目が品質からして網羅性があるものになっている。	10 以上	-
		机上デバグにおける摘出バクが一定の基準以下で品質が安定している。	100 以下	-
		工程毎バグ摘出件数が一定の基準以下で品質が安定している。	100 以下	20
	納期	工程毎の納期が達成できている。	95 以上	100
		納期毎の遅延が抑えられている。	5 以下	0
品質管理	品質	リリース後に発見されたバグの件数が想定される範囲内にある。	1 以下	0
	コスト	工程毎の開発要員及び工数が計画通りである。	100 以下	100

3.2. 本事業により開発したシステム

3.2.1. 開発したシステムの全体像について

医療認証基盤システムは、リクエスト受付サーバと認証サーバの 2 つの HW で構成する。

・ リクエスト受付サーバ
外部からのリクエストを受け付け、認証サーバに対して認証確認や認証アサーションの要求を行う。
参照クライアントより HPKI カードでの認証を行うためリクエストを受け付ける機能と医師資格確認サーバより SAML の認証アサーション要求の受け付ける機能をもつ。

・ 認証サーバ
利用者の認証情報を管理し、リクエスト受付サーバからの要求に応じて認証情報や SAML の認証アサーションを提供する。認証情報が含まれるため、インターネットからは直接アクセスせず、リクエスト受付サーバ経由でのアクセスを前提とする。
認証機能では、SAML 連携モジュール（サーバ）が組込まれており、SAML 連携モジュール（APP）からの要求に応じて認証アサーションを提供する機能をもつ。

医療認証基盤システムでは、安全性を担保するため冗長構成やセキュリティ対策を行う。

・ テープ装置を使ってシステムおよびデータのバックアップ・リストアを行なう
・ 各サーバにはウィルス対策ソフトウェアを導入してウィルスの侵入を阻止する

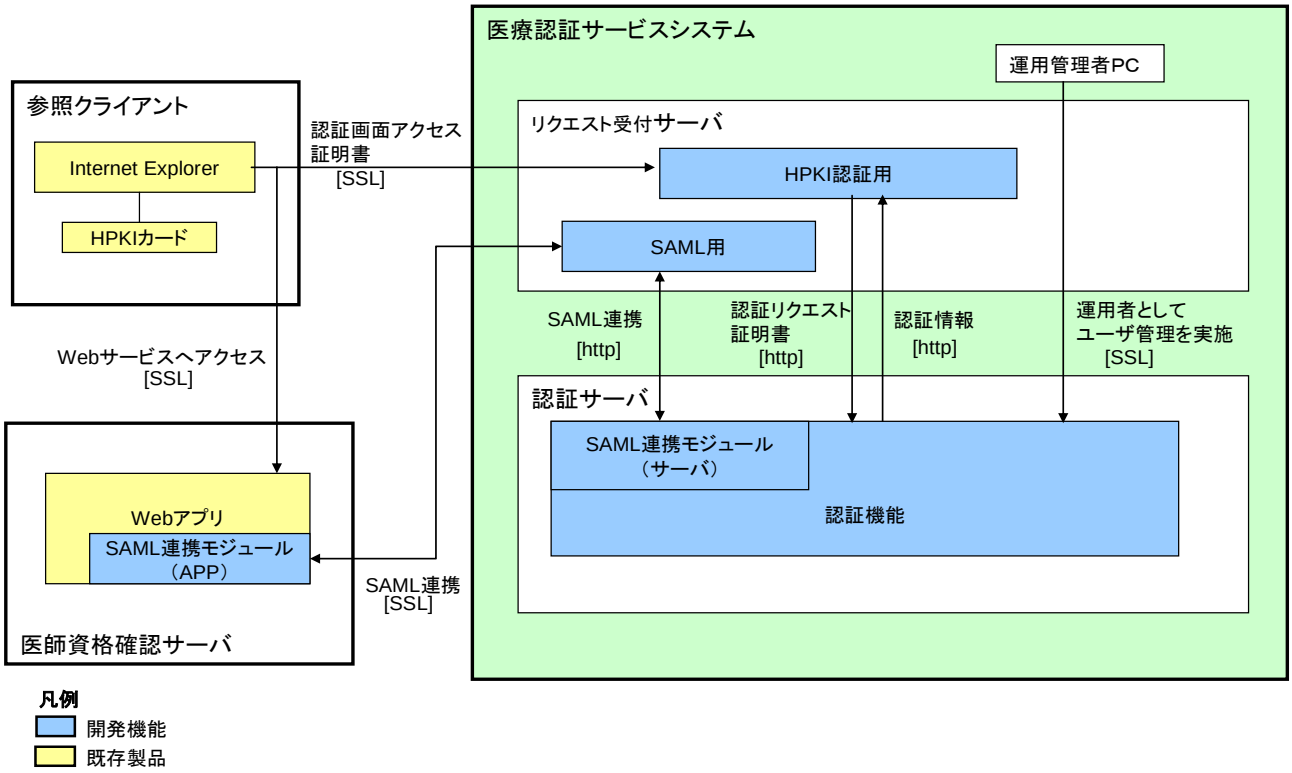


図 3.2.1-1 システム構成

3.2.2. アプリケーションシステムへの組込み方法

アプリケーションへ組込む SAML 連携モジュール（APP）として API 型のモジュールと AP 型のモジュールを提供する。

API 型のモジュールでは SAML 連携モジュール(APP)のモジュールおよび及び依存関係にある jar ファイルを医師資格確認サーバのアプリケーション内に組込むことで、JavaAPI を通して医籍番号・hcRole を提供する。

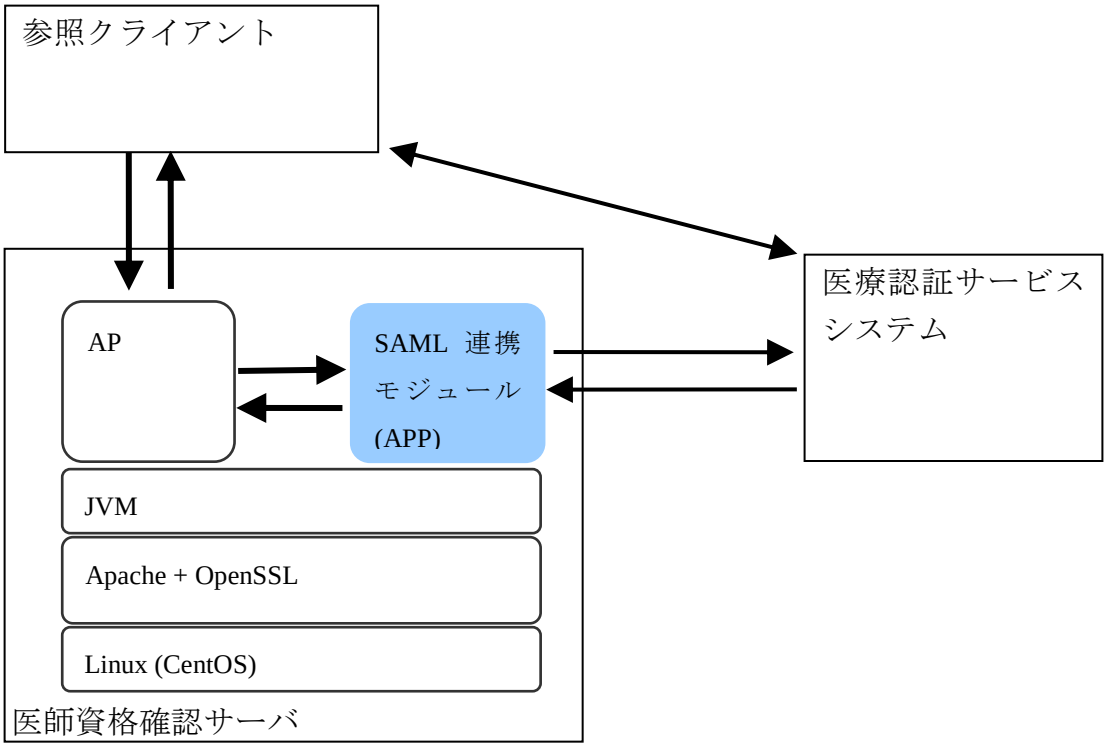


図 3.2.2-1 API 型のアプリケーション組込み方法

AP 型のモジュールでは医師資格確認サーバが参照クライアント（ブラウザ）と Web アプリケーションの間に入り、リバースプロキシとして動作する。参照クライアントから医師資格確認サーバと SSL 通信を行い、医師資格確認サーバと Web アプリケーションは http 通信を行う。また、医師資格確認サーバより、医療認証基盤システムに認証情報を問い合わせるため、医師資格確認サーバから医療認証基盤システムに SSL 通信を行う。

Web アプリケーションに対しては認証情報を http ヘッダーにて提供する。提供するヘッダーは以下のとおり。

・ SSO_USER：医籍番号
・ SSO_HCROLE：資格情報

Web アプリケーション側では上記ヘッダーに基づく処理を実装する必要がある。

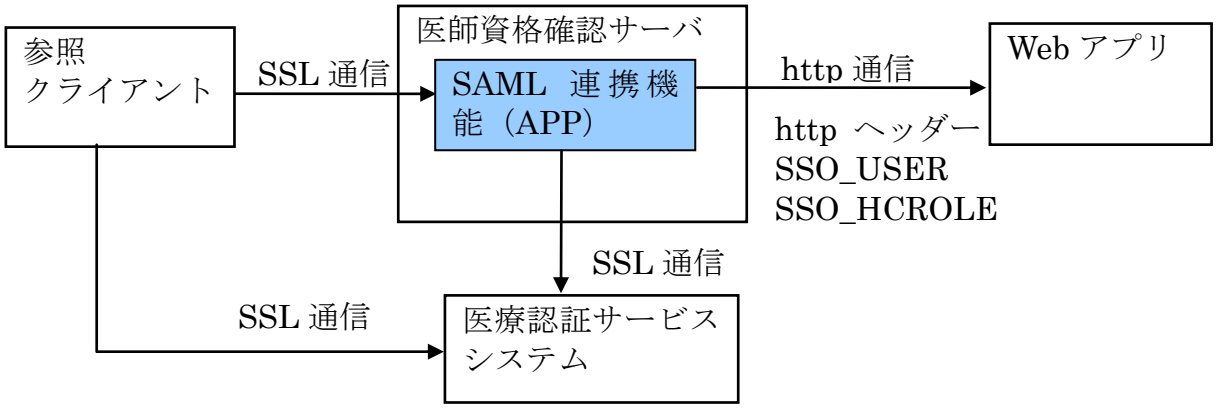


図 3.2.2-2 AP 型のアプリケーション組込み方法

3.2.3. 利用者管理方法

医療認証基盤システムの利用には、医療認証基盤システムへの利用者登録作業が必要となる。利用者登録は HPKI カードの発行と連動して行なう必要があり、利用者への登録については以下のフローとする。
※①②⑥の内容は日医認証局の業務内容であり、本実証事業の対象外である。

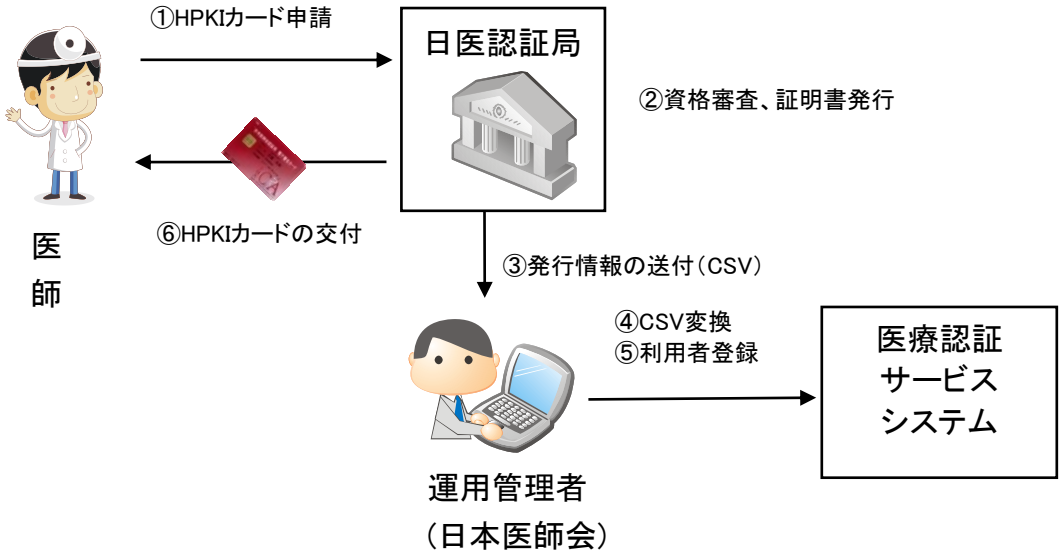


図 3.2.3-1 利用者の管理方法

3.2.4. サービス利用方法

一般利用者に対してのサービス利用方法を示す。

(1) 医師資格確認サーバ側にて認証前のページにアクセスし、認証が必要なページにリンクする（下記画面ではログインのボタンをクリックする）

図 3.2.4-1 利用画面（１）

(2) 医師資格確認サーバより医師の HPKI カードの認証を行うために医療認証基盤システムへリクエストが転送される。医療認証サービスでは、認証のために HPKI カードの証明書が必要となる。証明書を提供するため PIN 入力が表示されるため HPKI カードの PIN を入力する。

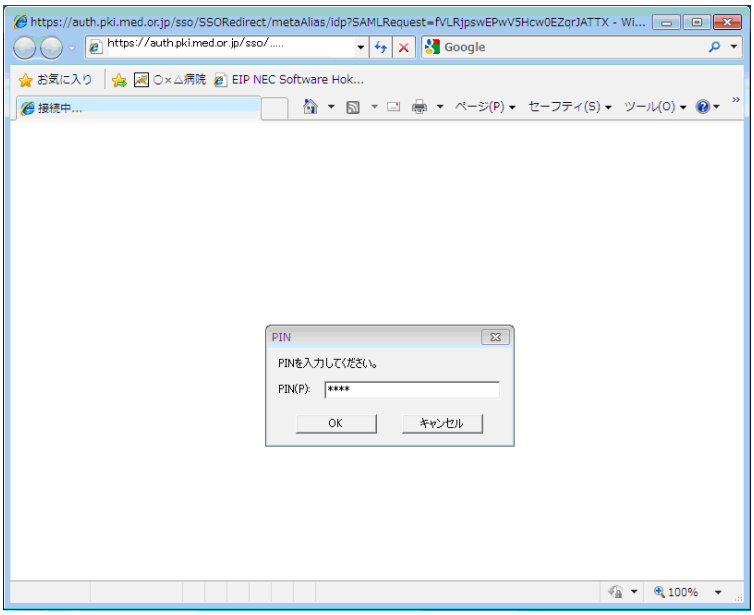


図 3.2.4-2 利用画面（２）

(3) 正しく PIN 入力されると医療認証基盤システムに HPKI カードの証明書が提供される。医療認証基盤システムでは証明書を元にユーザ認証が行われ、医師資格確認サーバに医籍番号と hcRole が認証情報として提供される。医師資格確認サーバ側で認証情報を元にアプリケーションの処理結果が表示される。

図 3.2.4-3 利用画面（３）

3.2.5. 運用方法

- 定期メンテナンスを除いてノンストップサービスを目指する。
- 集中監視センターからサーバの稼動状況を遠隔監視する。
- 医療認証基盤システムを冗長化によって障害によるデータ破壊やサービス停止を防ぐ。
- 障害時は速やかにリカバリできる体制を準備する。

3.2.6. データセンタの運用基準

医療認証基盤システムは、次のような基準のデータセンタにおいて運用する。

（1） 入退室管理

データセンタの入り口から機器設置エリアまでには、以下の 3 段階のセキュリティチェックを行う。

第 1 段階： 身分証明書提示による人による対面チェック
第 2 段階： 専用セキュリティカードによる入室管理
第 3 段階： 掌形認証と IC カードの組合せによるセキュアゾーンへの入退室管理

（2） 建物構造

・1981 年建築基準法の基準を満たし、耐震・防振等、構造上の安全性を考慮した建物である。
・建築基準法上の耐火建築物である。
・水害対策が施された建築物である。

（3） 電力設備

・電力会社からデータセンタ内に引き込まれたそれぞれ異なる 2 系統で受電する。
・停電時対応のため、UPS（無停電電源装置）及び自家発電装置による電力供給を行う。

（4） 集中監視センター

・データセンタ内に集中監視センターを設置する。
・集中監視センターでは専用オペレータが 24 時間 365 日常駐しており、サーバ機器やネットワーク機器が正常稼動しているかどうかを常時監視する。
・万が一障害を検知した場合は、速やかに障害連絡を行う。

（5） 地震対策

・ラックは架台により建物構造体へ固定して、移動、転倒防止措置を講じる。

4. まとめ

本事業では、どこでも MY 病院構想やシームレスな地域連携医療において、国民の医療・健康情報を安全に交換、流通させるために、以下の２つの事項の達成を目標とし、医療認証基盤システムとして HPKI 認証基盤環境を整備した。

・認証を一元化することで、利用者の利便性向上を実現する。

・国民の情報にアクセスしてよい資格者の確実な認証を実現する。

具体的には、医療情報化によって必要となる認証基盤として、厚生労働省の推進する保健医療福祉分野 PKI(以降、HPKI)を利用した医療認証基盤システムを構築するために必要となる「SAML 実装仕様書」の作成と、作成した「SAML 実装仕様書」に基づく、医療従事者の中で特に今回は医師の認証を実現する SAML 連携モジュールを開発し、医療情報化促進事業の他フィールドにおける開発や導入・構築負荷を低減可能とした。これらの成果物により HPKI 認証基盤環境の整備を行った。

本事業における SAML 連携モジュールは、SSL の標準的なパッケージや WEB ブラウザを活用して構築している。このため、PKI を用いて利用者認証を行う、医療以外のシステムへの展開も可能である。しかし、サイト間でアサーションの引継を行うプロトコルについては期間的な問題もあり検討の範囲外としたため、シングルサインオンよって複数のサイトが連携してサービスを提供するための十分な機能が提供できていない。このため、今後は第三者認証モデルに基づいたアサーションの引継方法に関する実装方法を具体的にする必要がある。

また、SAML を用いて認証を行うための最適な通信環境に関する要件について、期間的な制約により明確にすることが十分にできていない。このため、今後はさらにシステム分析を詳細に行って、SAML や認証に適した通信環境を明らかにしていく必要がある。

また、本事業で適用した実証フィールドでは、利用者認証を厚生労働省の HPKI に基づいて行い、クライアントとサーバの接続認証には VeriSign を共通のトラストポイントとして採用し認証を行った。このようなトラストポイントとなり得る民間の PKI の認証局は複数存在し、必ずしも共通のトラストポイントが存在しない。このため、今後本事業の成果のような認証システムを普及させるには、保健医療福祉分野として信頼できるトラストポイントの確立が不可欠と考える。今回の検討範囲では利用しなかったが、HPKI には人だけでなく、組織を認証する仕組みも提示されており、認証局を立ち上げることによって、保健医療福祉分野で安全なネットワークを構築するための認証のトラストポイントとなることが期待される。このため、HPKI に基づいたクライアントとサーバ間のクライアント認証に関わる保健医療福祉分野のトラストポイントを構築するように働きかけていきたい。

今後の普及展開へ向けた課題を下記に挙げる。

・全国へ向け普及し、持続可能なサービスとして定着が図れるか
・医師以外の様々な国家資格（薬剤師、歯科医師、看護師等）に関して普及が図れるか
・国家資格以外の介護・福祉従事者や行政職員等への展開が図れるか

第一の点に関しては、本事業の成果は、我が国の保健医療福祉分野におけるセキュリティ対策として、各地で展開されている「シームレスな地域連携医療」や「どこでも My 病院事業」等や、既存の医療連携サービスにも適用可能なものであり、標準化された技術（たとえば SS-MIX 標準化ストレージなど）と組み合わせた形で広く活用いただき、標準的な医師の認証サービスとして浸透できるよう普及啓発活動に努めたい。また、今後も日本医師会が公益事業として認証サービスを運用していくことにより、公正中立な立場での全国規模での展開が容易となるため、具体的な形で活用され普及していくことが大いに期待される。

第二の点に関しては、本事業で開発した、SAML 連携モジュールは、「HPKI の Subject の DN-ID に医師の医籍番号に相当する ID を設定する」ことによって、様々な国家資格（薬剤師、歯科医師、看護師等）に対応した利用者認証を提供することができる。しかし、現在はこれら医師以外の資格を使ったサービスやサービスのための認証局は世の中にない。本事業の成果により技術面、運用面におけるひな型が整備・提示できたと考えており、導入に向けたハードルが低くなり、医療全体の基盤となる認証システムとして各団体における議論が活性化されることが期待される。

第三の点は、現在の医療従事者等に発行する HPKI は、国家資格を保有している人を対象としているため、保健医療福祉分野の現場で関わる従事者を対象にできるか、発行方法をどうするか等も含め、HPKI 全体の在り方として検討していくことが期待される。

最後に、本事業は検討期間等の制約があり、あくまでも「医師」に限定した認証サービスを各地に展開する「第一歩」として実現したものである。 本事業の成果を、「医師」から、保健医療福祉分野の現場に携わる従事者まで展開するために、国としての保健医療福祉分野の基盤の普及促進に向け進んでいきたい。